User Manual

WBR-5050

Wireless 802.11n Dual Band
Broadband **Router**

LG-ERICSSON

1. Introduction 6
1.1. Package Contents 6
1.2. System Requirements 6
1.3. Introduction 7
1.4. LED Overview 8
1.5. Before you Begin 9
2. Configure PC/Laptop Network Interface 10
2.1. Windows XP/Vista 10
2.2. Windows 7 13
2.3. Apple Mac OS X 15
3. Setup your Router 16
4. Manually enter Setup Wizard 19
5. System 32
5.1. Status 32
5.2. LAN (Local Area Network) 36
5.3. DHCP 40
5.4. Schedule 43
5.5. Log 45
5.6. Monitor 46
5.7. Language 47

6. Internet 48
6.1. Status 48
6.2. Dynamic IP Address (DHCP) 49
6.3. Static IP Address 51
6.4. PPP over Ethernet (PPPoE) 52
6.5. Point-to-Point Tunneling Protocol (PPTP) 54
7. Wireless 2.4G 56
7.1. Basic 56
7.2. Advanced 59
7.3. Security 61
7.4. Filter 67
7.5. Wi-Fi Protected Setup (WPS) 69
7.6. Client List 72
8. Wireless 5G 73
8.1. Basic 73
8.2. Advanced 75
8.3. Security 77
8.4. Filter 78
8.5. Wi-Fi Protected Setup (WPS) 80
8.6. Client List 81

9. Firewall....82
9.1. Enable....82
9.2. Advanced....83
9.3. DMZ (Demilitarized Zone)....84
9.4. Denial of Service (DoS)....85
9.5. MAC Filter....86
9.6. IP Filter....87
9.7. URL Filter....89
10. Advanced....90
10.1. Network Address Translation (NAT)....90
10.2. Port Mapping....91
10.3. Port Forwarding....93
10.4. Port Trigger....94
10.5. Application Layer Gateway (ALG)....95
10.6. Universal Plug and Play (UPnP)....96
10.7. Quality of Service (QoS)....97
10.8. Routing....100
11. Tools....101
11.1. Admin....101
11.2. Time....102

11.3. Dynamic DNS (DDNS) 103
11.4. Diagnosis 104
11.5. Firmware 105
11.6. Back-up 108
11.7. Reset 109
Appendix A – FCC Interference Statement 110
Appendix B – IC Interference Statement 112

Revision History

Version	Date	Notes
1.0	2011/08/04	First Release

1. Introduction

1.1. Package Contents

- The LG-Ericsson WBR-5050 Dual Band Concurrent Wireless 802.11n Broadband Router
- AC Power Adapter
- RJ-45 Ethernet LAN Cable
- CD-ROM with User Manual
- Quick Installation Guide

If any of these items are incorrect, missing, or damaged, contact your reseller or distributor. Keep the original package contents in case you need to return the product for repair or replacement.

1.2. System Requirements

- RJ-45 Ethernet Based Internet (ADSL or Cable Modem)
- Computer with Wireless Network function
- Windows, Mac OS or Linux based operating systems
- Internet Explorer, Firefox or Safari Web-Browser Software

1.3. Introduction

The LG-Ericsson WBR-5050 Wireless 802.11n Dual Band Broadband Router is the ideal solution for providing high speed wireless to your home or home office. The WBR-5050 con-nects PCs, wireless printers, gaming consoles, and other Wi-Fi devices at transfer speed up to 300Mbps per frequency band. The WBR-5050 supports simultaneous dual band op-eration to provide the maximum throughput for file transfers, HD video streaming, and on-line gaming. With the 2.4GHz frequency band becoming more and more crowded the ability to operate in the 5GHz band helps avoid interference and optimize wireless performance for bandwidth intensive multimedia applications. MIMO (Multiple-In, Multiple-Out) antenna technology provides enhanced wireless coverage so you can enjoy wireless connectivity anywhere in your home.

With WPA/WPA2 encryption and SPI firewall, the WBR-5050 Router helps keep the network protected. The Router also supports Wi-Fi Protected Setup (WPS) for simple and secure wireless connections. In addition, the WBR-5050 supports up to four SSIDs per frequency band to provide separate access and security restrictions for home and guest users.

Combining multiple connections with high speed and flexible security, the LG-Ericsson WBR-5050 provides the maximum reliability and security to your home and home office.

1.4. LED Overview

LED Lights	Icon	Description
WPS		Off – WPS is not enabled. Solid White for 300 seconds – WPS process is running. Blinking White –WPS handshake is initialized.
Power		Off – The router is not powered on. Solid Orange – The router is powered on. Blinking Orange – Reset is in process.
Wireless LAN 2.4GHz		Off – The wireless 2.4GHz radio is off. Solid Blue - The wireless 2.4GHz radio is activated and is available. Blinking Blue – The wireless 2.4GHz radio is transmitting or receiving data.
Wireless LAN 5GHz		Off – The wireless 5GHz radio is off. Solid White - The wireless 5GHz radio is activated and is available. Blinking White – The wireless 5GHz radio is transmitting or receiving data.
Internet		Off – The router is not connected to the Internet (DSL/Cable modem). Solid Blue – The router is connected to the Internet. Blinking Blue - The Internet port is transmitting or receiving data.
LAN (Ports 1-4)		Off – No link is detected on the port. Solid Blue – The LAN port has detected a link with an attached network device. Blinking Blue – The LAN port is transmitting or receiving data.

1.5. Before you Begin

The operating distance or range of your wireless connection can vary significantly depending on the placement of the Router. For best performance:

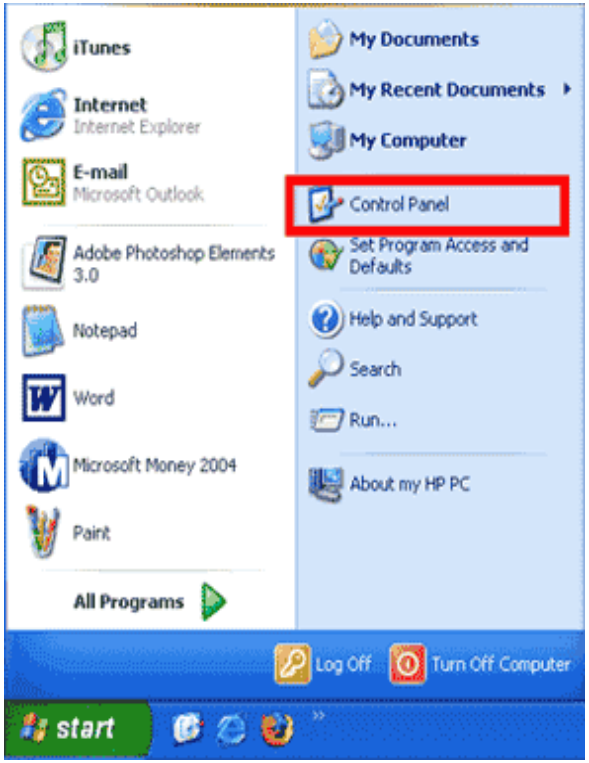
- Place the Router near the center of the area where your computers and other network devices will operate.
- Keep the number of walls and ceilings between the Router and the wireless devices to a minimum.
- Keep the Router away from electrical devices which are potential sources of interference, such as microwaves, cordless phones, etc.
- Avoid placing the Router on or near metal objects (such as a solid metal door, file cabinets, metal furniture) and reflective surfaces (such as glass or mirrors)
- Avoid placing the Router in enclosed spaces such as a closet, cabinet or wardrobe.
- Minimize obstructions between the Router and the wireless devices. Any obstruction, even non-metallic objects, can weaken the wireless signal.

If your wireless signal is weak, try placing the Router in several locations and test the signal strength to determine the best position.

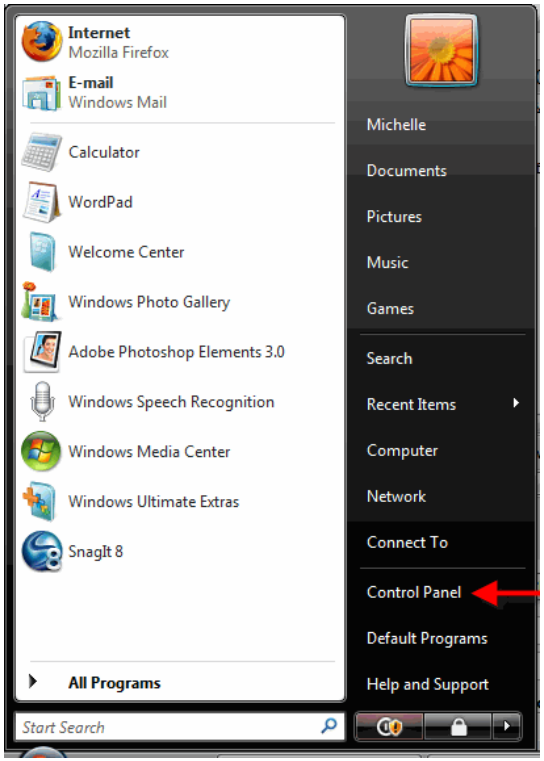
2. Configure PC/Laptop Network Interface

2.1. Windows XP/Vista

- Click Start button and open Control Panel.



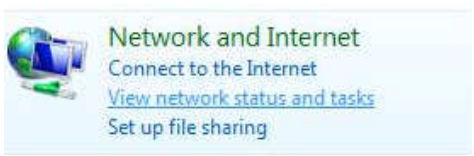
Windows XP

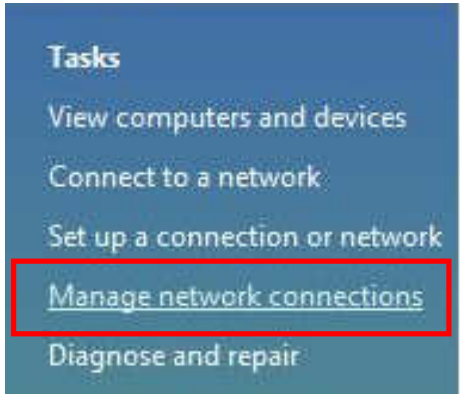


Windows Vista

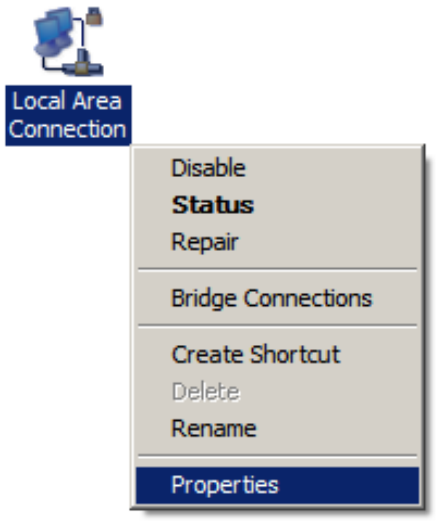
- Windows XP, click [**Network Connection**]

- Windows Vista, click [**View Network Status and Tasks**] then [**Manage Network Connections**]



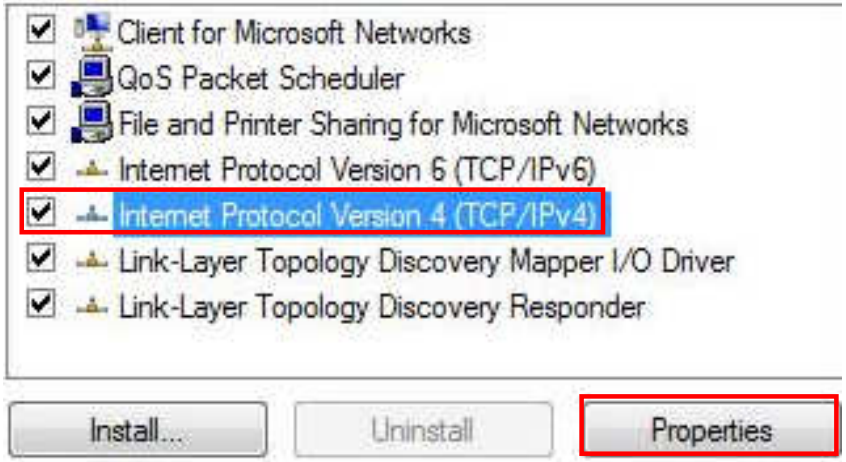


- Right click on [**Local Area Connection**] and select [**Properties**].



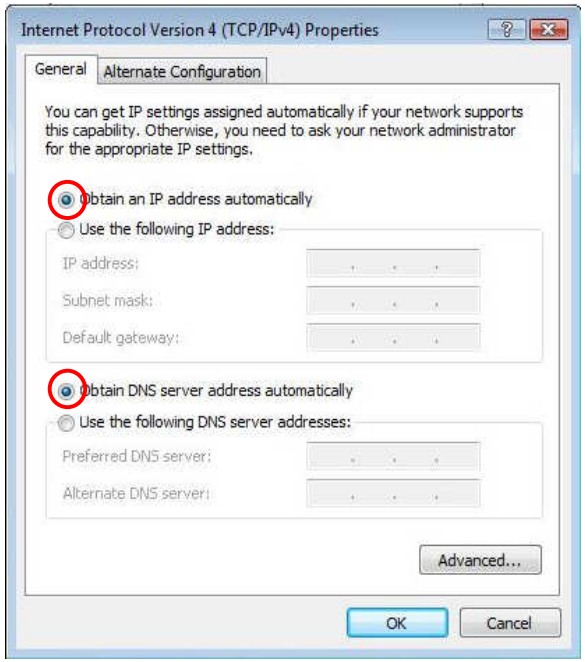
- Make sure the boxes "**Client for Microsoft Networks**", **"File and Printer Sharing**", and "**Internet Protocol (TCP/IP)**" are checked. If not, please install them.

- Select "**Internet Protocol (TCP/IP)**" and click [**Properties**]



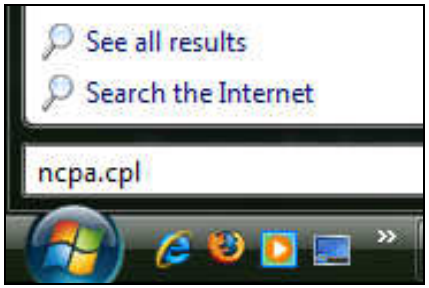
- Select **Obtain an IP Address automatically** and **Obtain DNS** server **address automatically**

- Click **OK** to complete

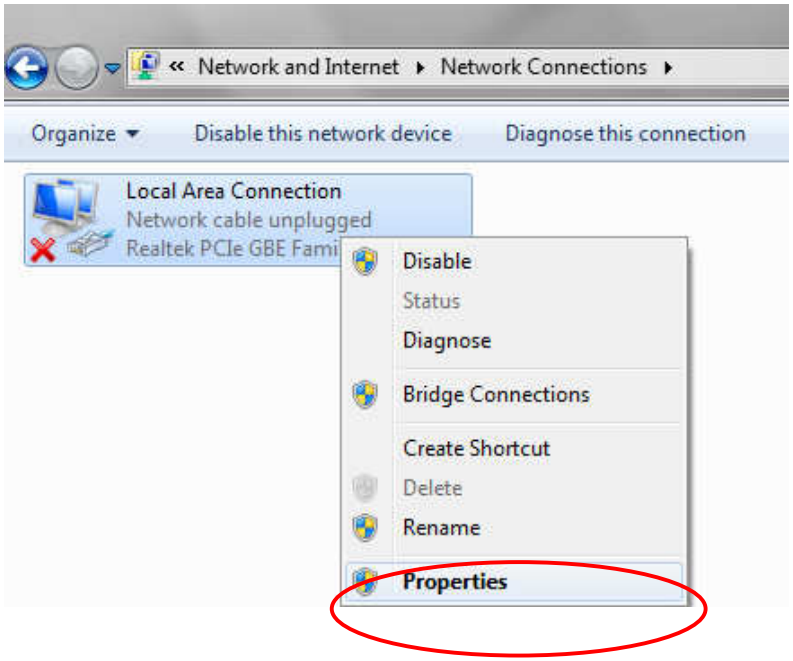


2.2. Windows 7

- In the **Start** menu search box, type: **ncpa.cpl**

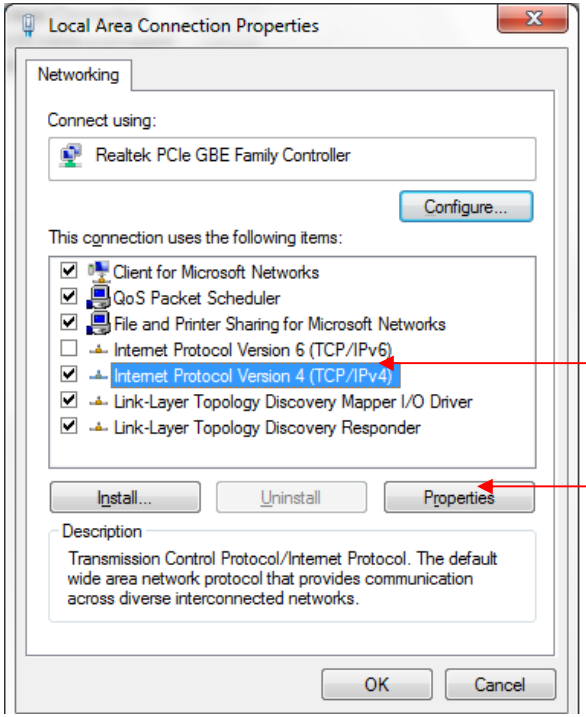


- The Network Connections List appears.



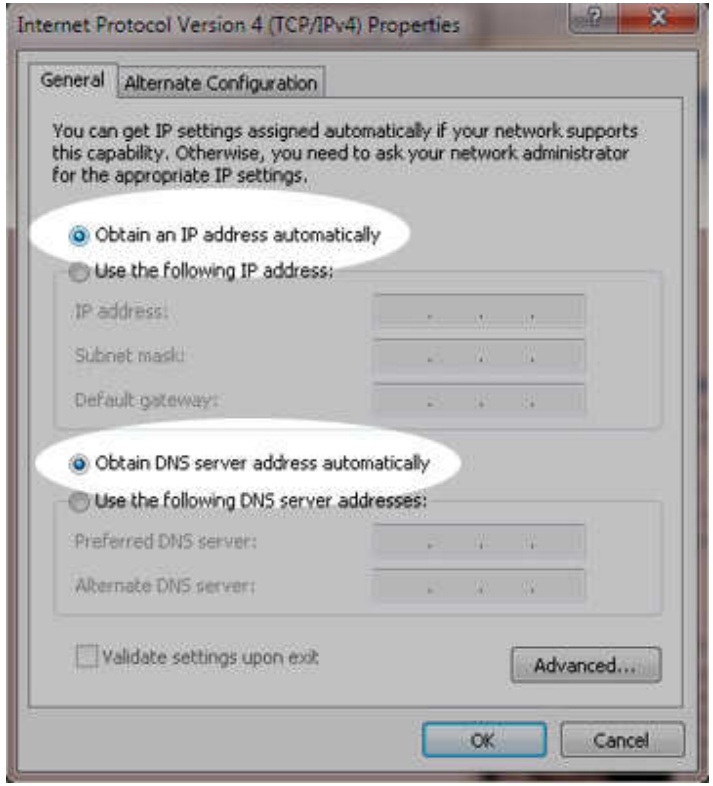
- Right-click the **Local Area Connection** icon and click **Properties**.

- In the Networking tab of the **Local Area Connection Properties** dialog box, click either **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.



Internet Protocol Version 4 (TCP/IPv4)

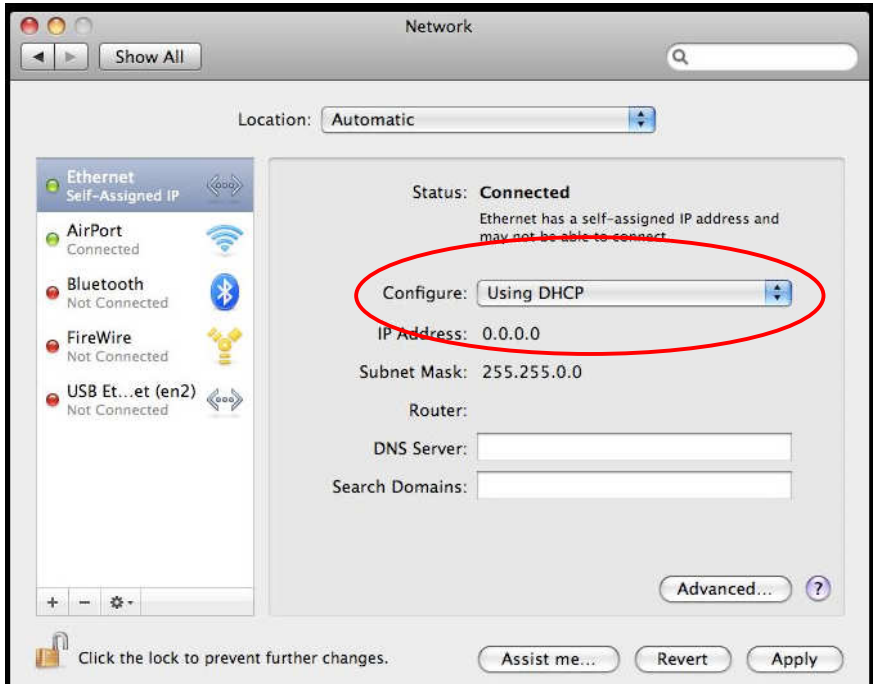
Properties Button



- Select **Obtain an IP Address automatically** and **Obtain DNS server address automatically**.
- Click **OK** to complete.

2.3. Apple Mac OS X

- Go to **System Preferences** > **Network**.



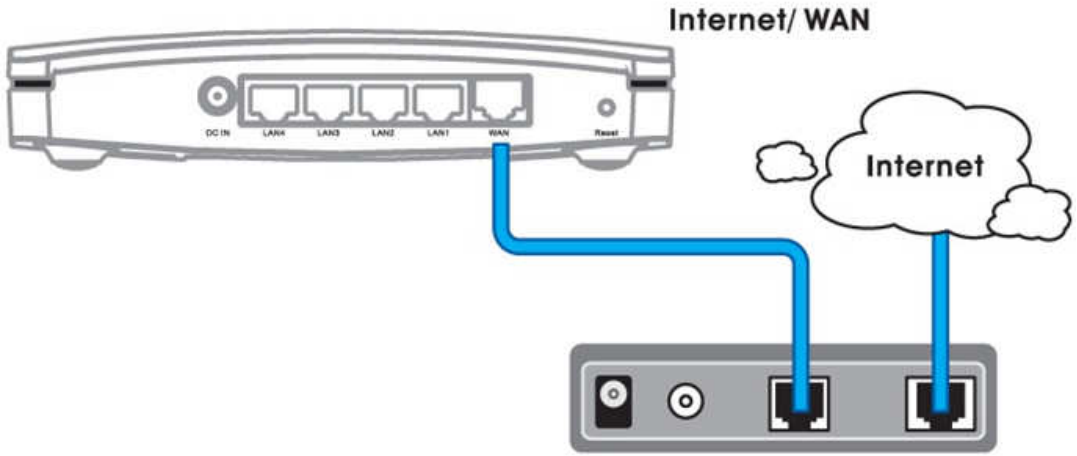
- Under Network setting, select **Using DHCP**.
- Click **Apply** when done.

3. Setup your Router

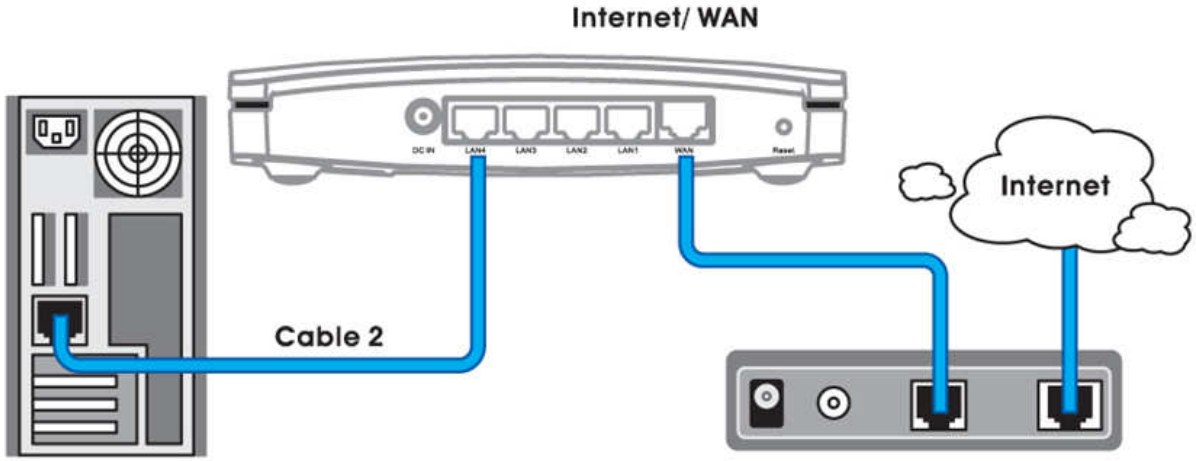
Follow the instructions below to setup your Router.

Or, you may follow the instructions on the LG-Ericsson Installation Wizard for basic setup: Insert the Installation CD into the CD-ROM drive on your desktop or laptop. The CD will automatically start. The LG-Ericsson Installation Wizard will pop up. Click on **Quick Setup** and follow the onscreen instructions for hardware installation.

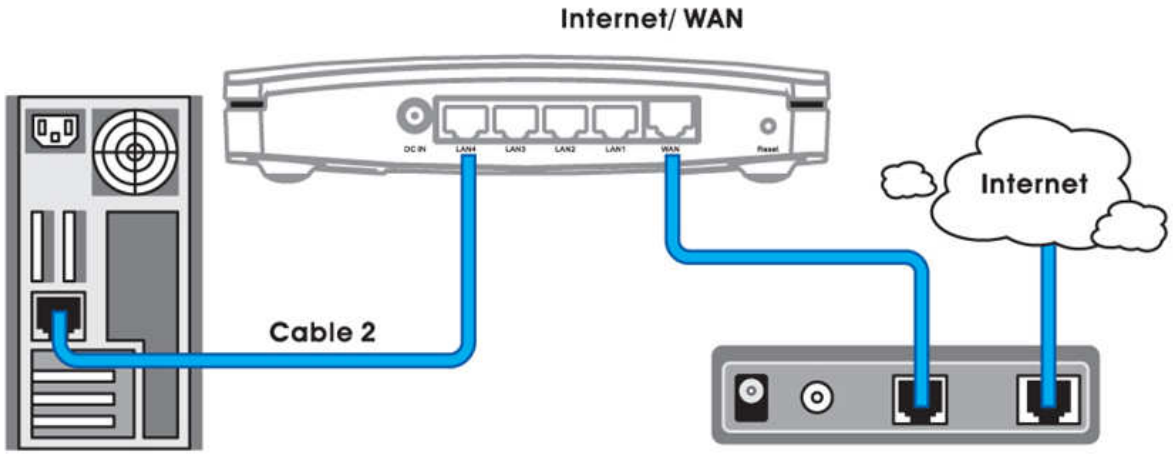
1. Plug in the adapter
2. Please wait until Wireless LED is on



3. Connect modem and router with an Ethernet cable as shown above



4. Please configure your network interface to DHCP (obtain an IP address automatically)
5. Connect PC/Laptop and the router with an Ethernet cable as shown above (Cable 2)



6. Please check your Ethernet cable setting again and make sure it is the same as shown above
7. When confirmed, please click [Next] to enter Wizard setup

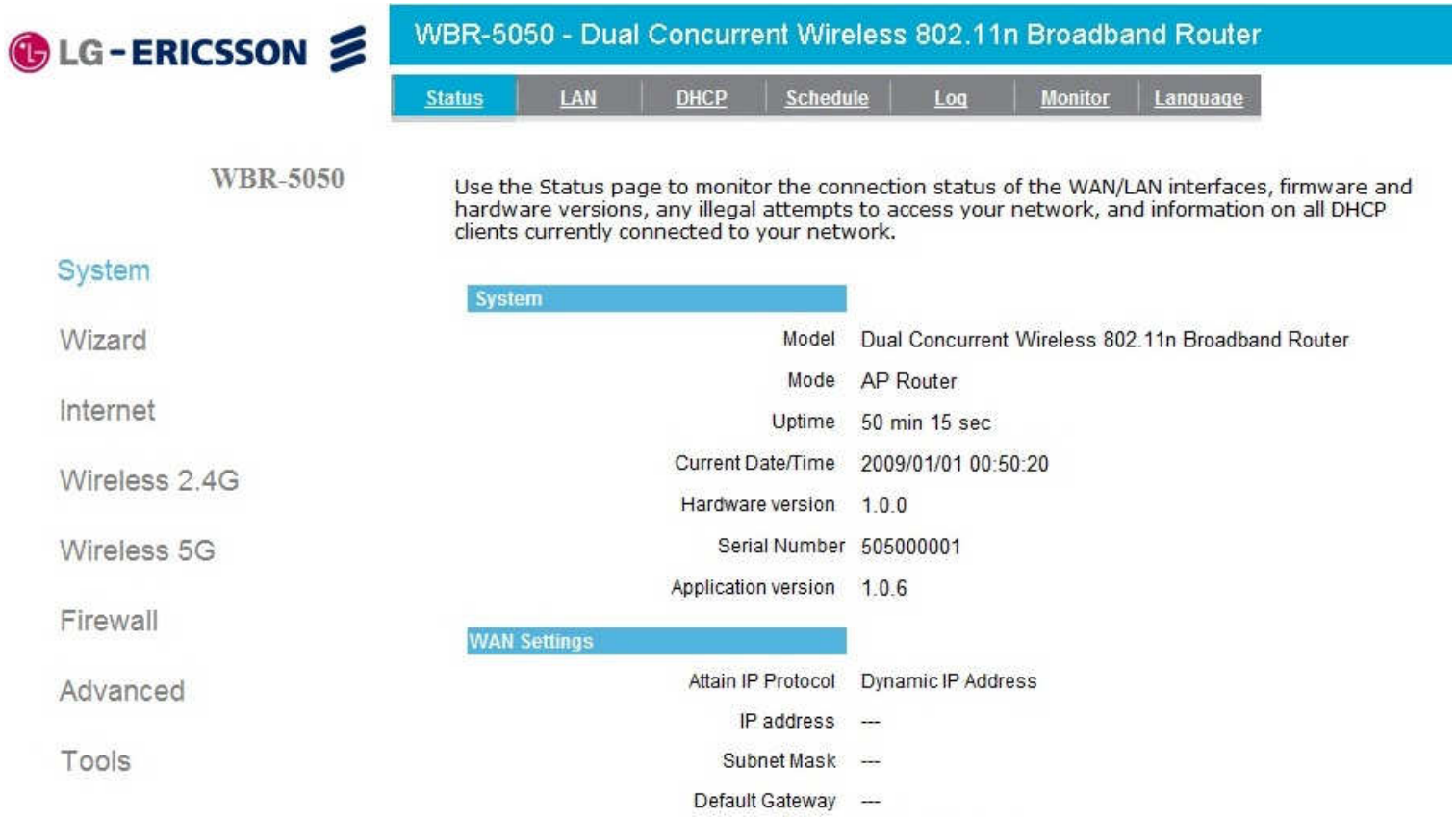
4. Manually enter Setup Wizard

1. Open a web browser (Internet Explorer/Firefox/Safari) and enter the address http://192.168.2.1

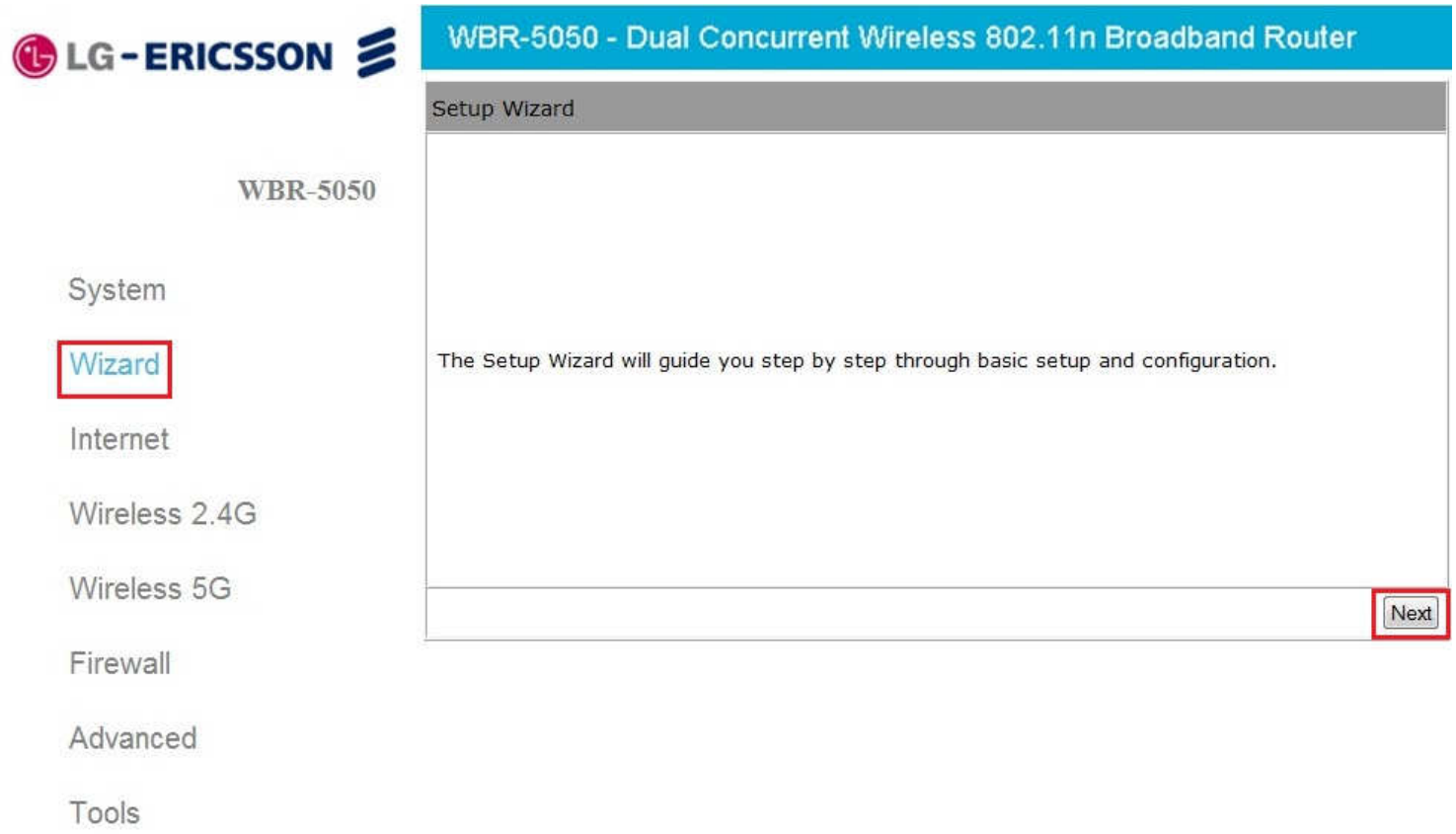
   Note: If you have changed the default LAN IP Address of the WIRELESS ROUTER, make sure that you enter the correct IP Address.

2. The default username and password are **admin** and **admin**. Once you have entered the correct username and password, click the **LOGIN** button to open the Web-based main menu.

3. You will see the following webpage if login successful.

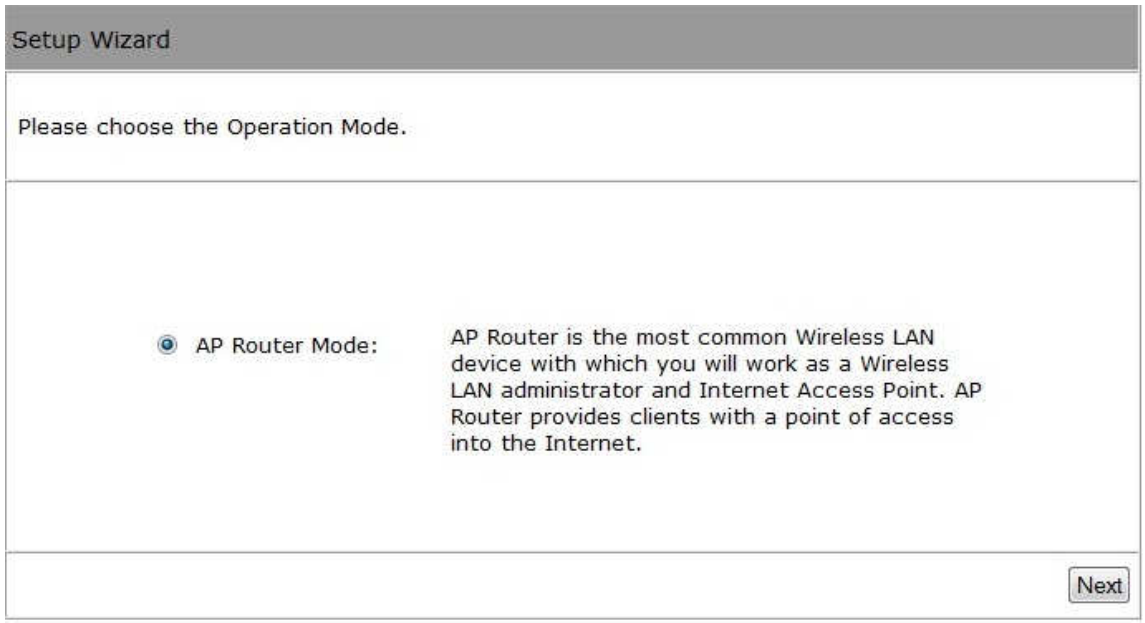


4. Click **Wizard** on the left menu to open the Setup Wizard. Click **Next** to begin the Wizard.



5. Select the Operation Mode.

Make sure you have the proper cables connected as described in the Setup your Router section.



AP Router Mode

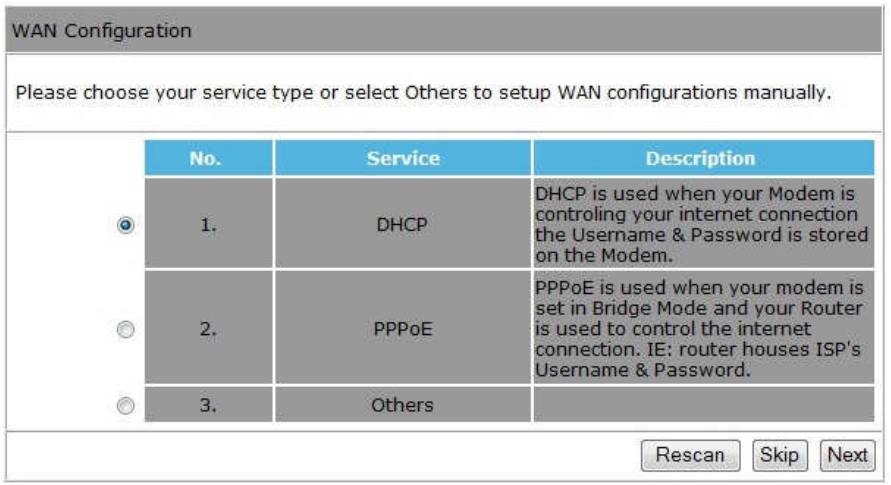
a) The Router will now automatically search for the correct WAN (Internet) settings.

b) The most appropriate WAN type will be determined and selected automatically. If the detected type is incorrect, select **Others** to set up the WAN settings manually.

Note:

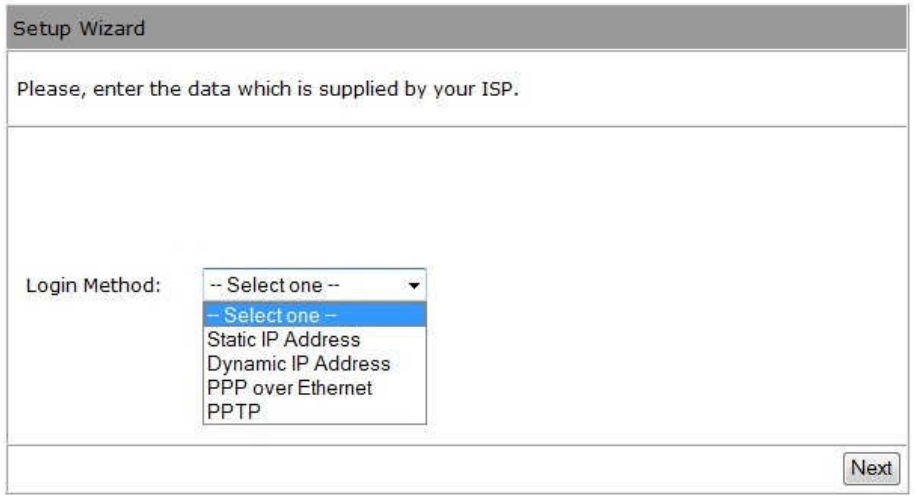
DHCP is for Cable connections.

PPPoE is for DSL connections.



c) There are many WAN service types available. Obtain the correct settings from your Internet Service Provider (ISP).

Note:
Choose **Dynamic IP Address** (DHCP) if you have a Cable connection.
Choose **PPP over Ethernet** (PPPoE) if you have a DSL connection.



Static IP Address

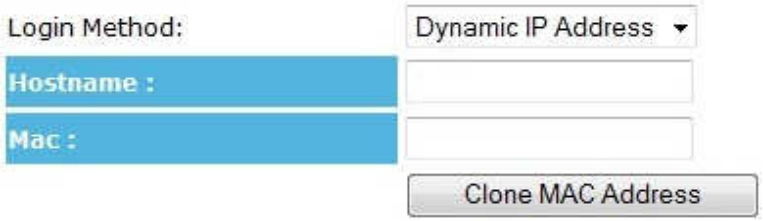
Select this option if your Internet Service Provider (ISP) has assigned you a permanent, fixed (static) IP address. Enter the IP address assigned by your ISP, subnet mask, default gateway IP address, and the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, also enter the address here.

Dynamic IP Address (DHCP)
Select this option if your ISP assigns an IP address dynamically by DHCP (i.e. Cable connections).

Typically, you can leave the Hostname and MAC address fields empty.

However, some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will only accept traffic from the MAC address of that computer.

If your ISP has registered the MAC address of your computer's Ethernet LAN card, connect only the computer with the authorized MAC address and click the **Clone MAC Address** button. This function allows your router to clone the authorized MAC address of the registered computer. The correct MAC address will be used to initiate the connection to the ISP.

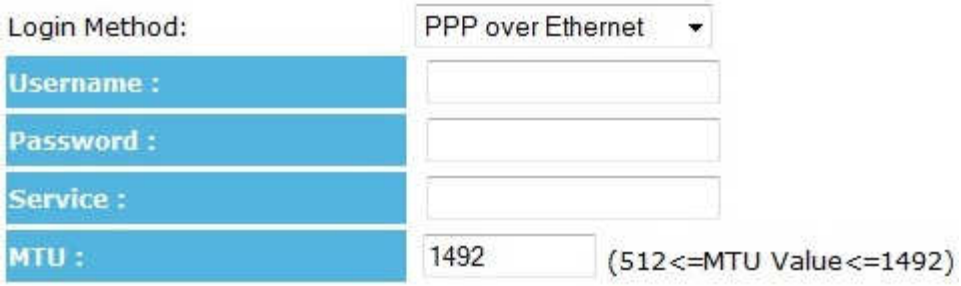


Dynamic IP Address	
Hostname	This is optional. Only required if specified by ISP
MAC	The MAC address that is used to connect to the ISP.

PPP over Ethernet (PPPoE)

This protocol is used by most DSL services worldwide. Select this option if you have a DSL connection.

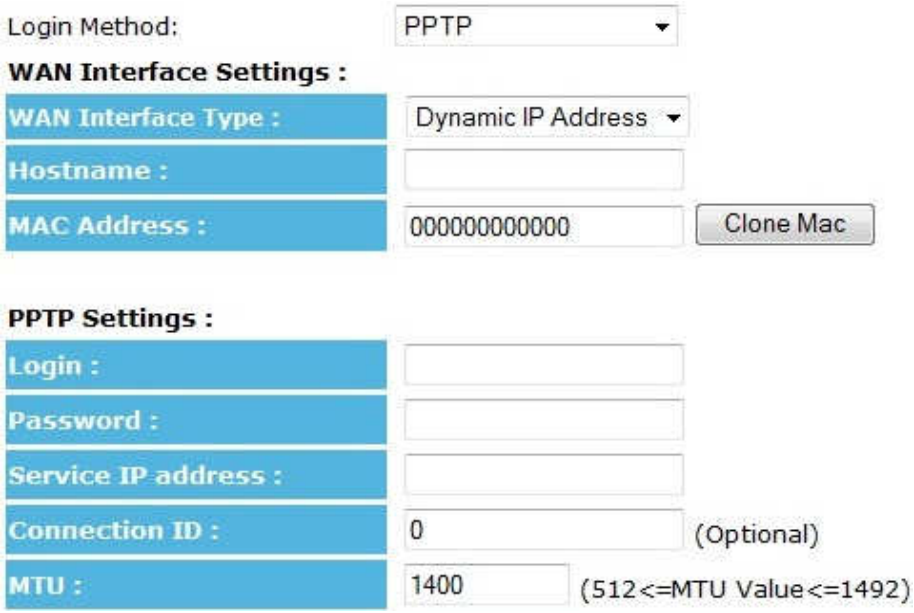
Enter the username and password provided by your ISP.



PPP over Ethernet	
Username	Username assigned to you by the ISP
Password	Password for this username.
Service	You can assign a name for this service. (Optional)
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.

Point-to-Point Tunneling Protocol (PPTP)

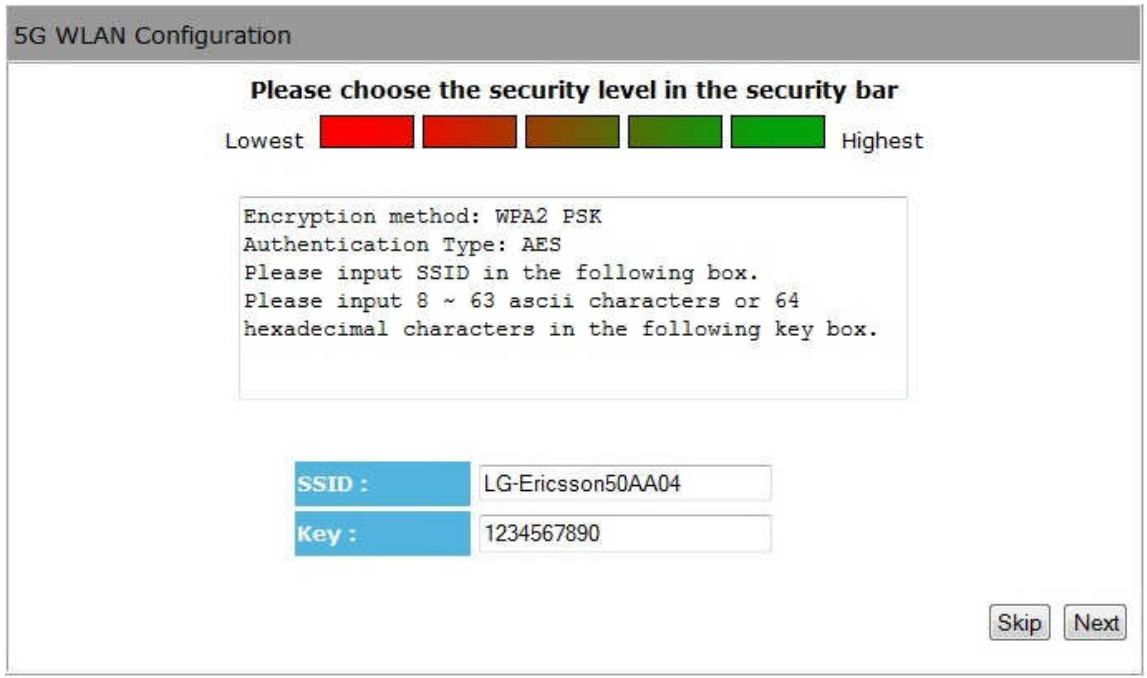
PPTP is used by a few ISPs. It is used primarily in Austrian DSL services.



PPTP	
WAN Interface Type	Select whether the ISP is set to Static IP or Dynamic IP addresses.
Hostname	This is optional. Only required if specified by ISP
MAC	The MAC Address that is used to connect to the ISP.
PPTP Settings	
Login	Username assigned to you by the ISP
Password	Password for this username.
Service IP Address	The IP Address of the PPTP server.
Connection ID	This is optional. Only required if specified by ISP
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.

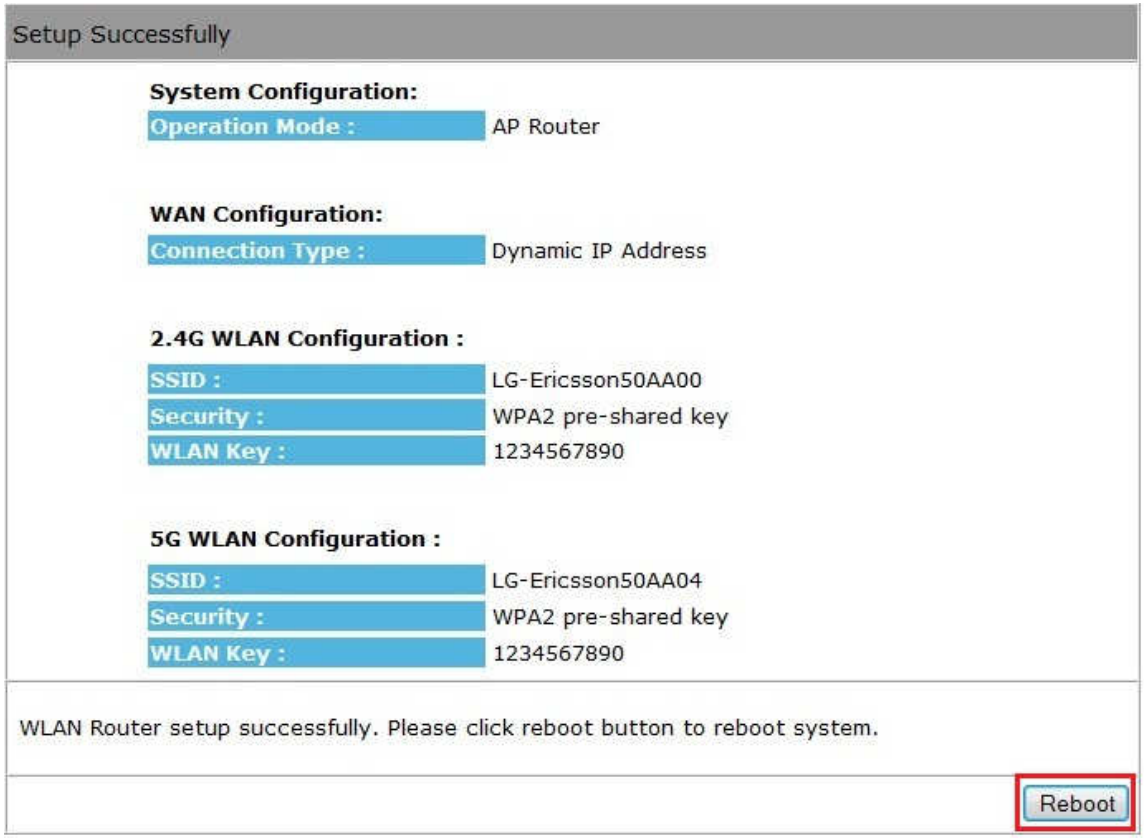
d) Setup the level of wireless security to be used.
LG-Ericsson recommends the **Highest** level of security to be used (**WPA2 PSK** as the Encryption method and **AES** as the Authentication type)

Note: 802.11n wireless speeds may not be achievable if the security is setup as the Lowest and Low levels.



SSID	Enter the name of your wireless network.
Key	Enter the security key for your wireless network.

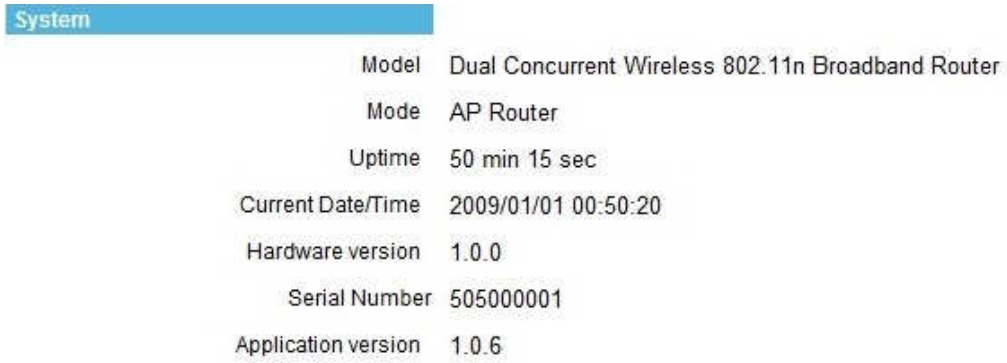
e) Make sure the settings are correct. Click **Reboot** to apply the settings.



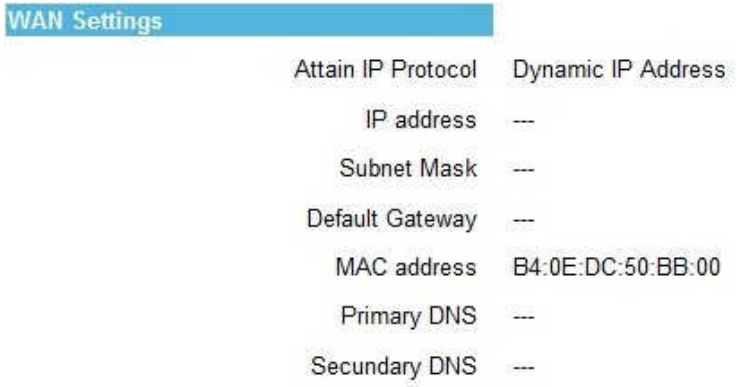
5. System

5.1. Status

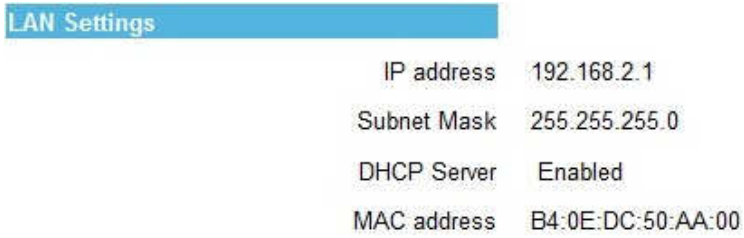
This page allows you to monitor the status of the Router.



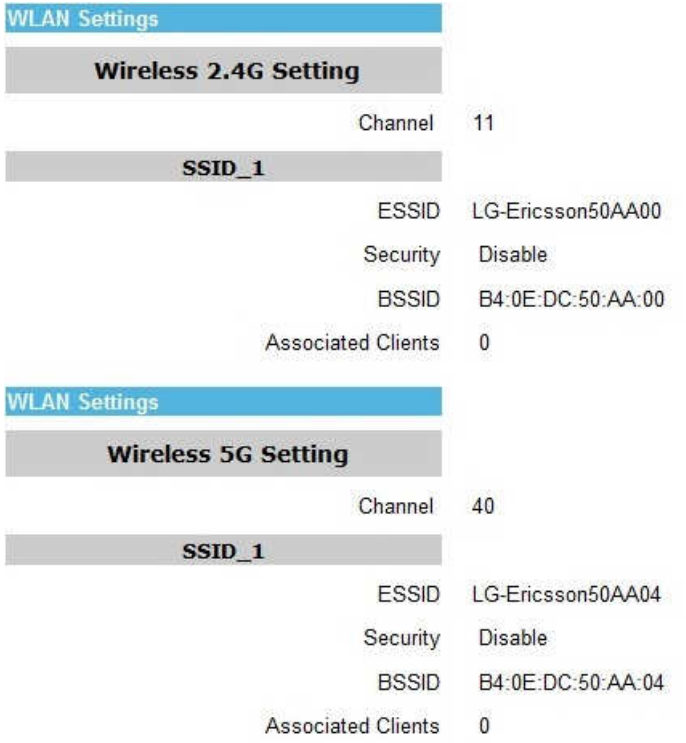
System	
Model	Description of the Router.
Mode	Operation mode of the Router.
Uptime	The duration of time that the Router has been operating.
Current Date/Time	The system time of the Router. If this is incorrect, you can set the correct time in the Tools / Time page.
Hardware version and Serial Number	Hardware information of the Router.
Application version	Firmware version of the Router.



WAN Settings	
Attain IP Protocol	Method used to connect to the Internet. This is your WAN connection type.
IP address	The WAN IP address of the Router.
Subnet Mask	The WAN subnet mask of the Router.
Default Gateway	The default gateway of the Router.
MAC address	The WAN MAC address of the Router.
Primary and Secondary DNS	The IP addresses of the Primary and Secondary DNS servers assigned to the WAN connection.



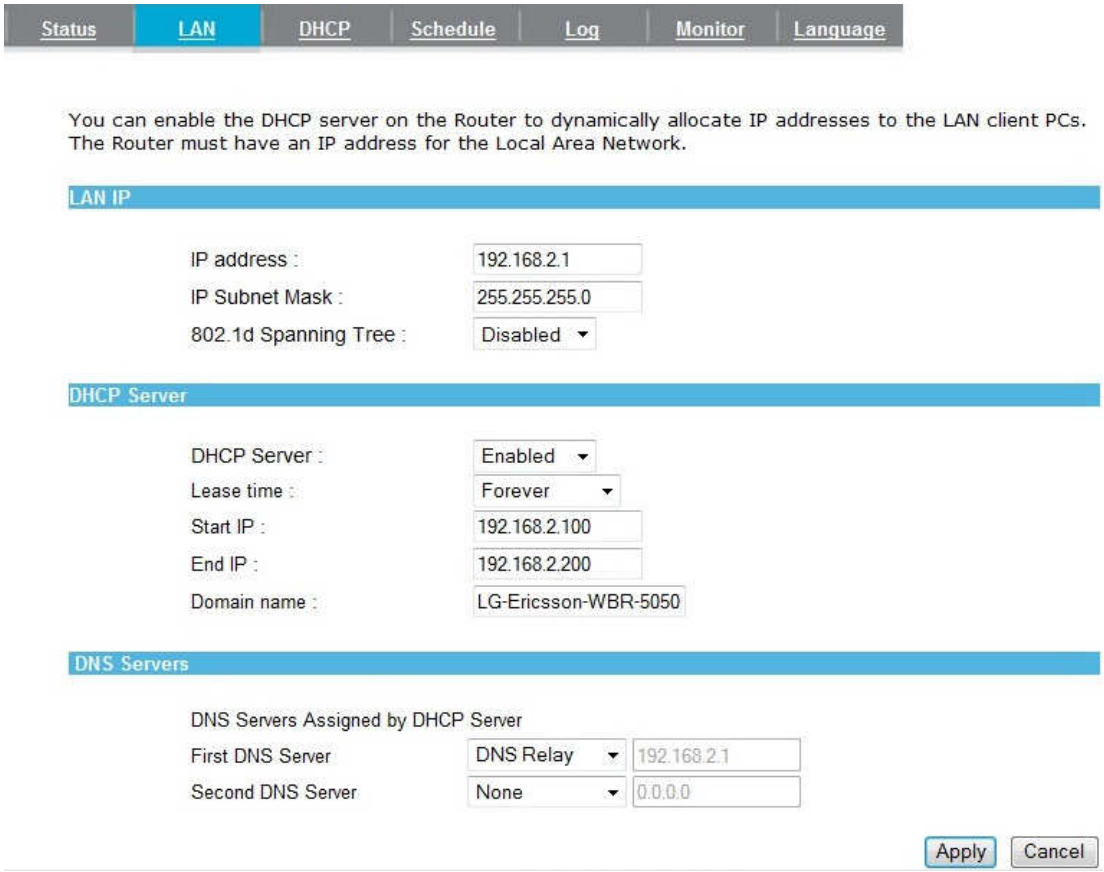
LAN Settings	
IP address:	The LAN IP Address of the Router.
Subnet Mask	The LAN Subnet Mask of the Router.
DHCP Server	Whether the DHCP server is Enabled or Disabled.
MAC address	The LAN MAC address of the Router.

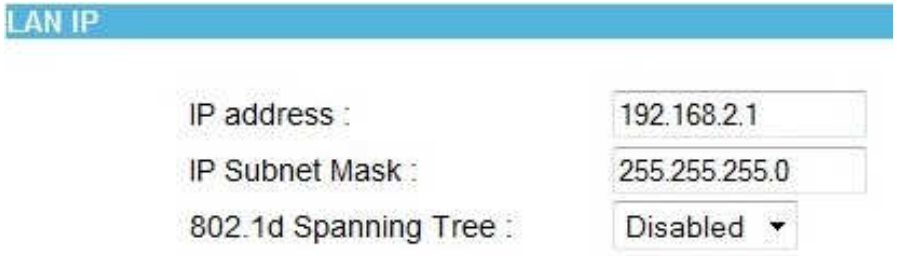


WLAN Settings	
Channel	The wireless channel currently in use.
ESSID	The SSID (Network Name) of the wireless network. (The WBR-5050 supports up to 4 SSIDs for each radio/frequency band)
Security	The type of wireless encryption enabled.
BSSID	The MAC address of this SSID.
Associated Clients:	The number of wireless clients connected to this SSID.

5.2. LAN (Local Area Network)

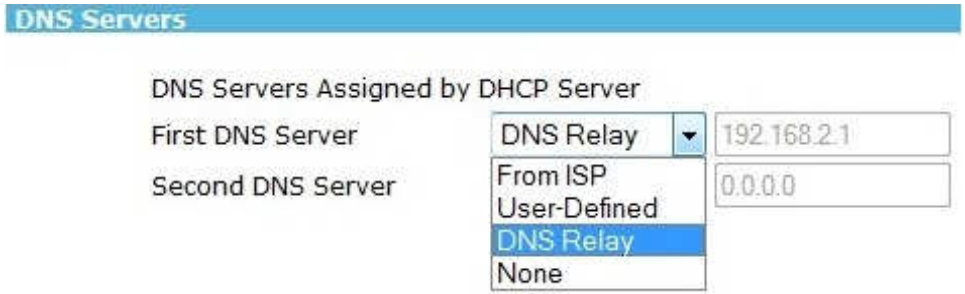
This page allows you to modify the LAN settings of the Router.





LAN IP	
IP address	The LAN IP Address of the Router.
IP Subnet Mask	The LAN Subnet Mask of the Router.
802.1d Spanning Tree	When Enabled, the Spanning Tree Protocol (STP) will prevent network loops in your LAN network. Default: Disabled.

DHCP Server	
DHCP Server	The DHCP Server automatically allocates IP addresses to your LAN devices. Default: Enabled.
Lease Time	The amount of time that a computer may have an IP address before it is required to renew the lease. Default: Forever.
Start / End IP	The range of IP addresses that the DHCP server will allocate to LAN devices.
Domain name	The domain name for this LAN network.

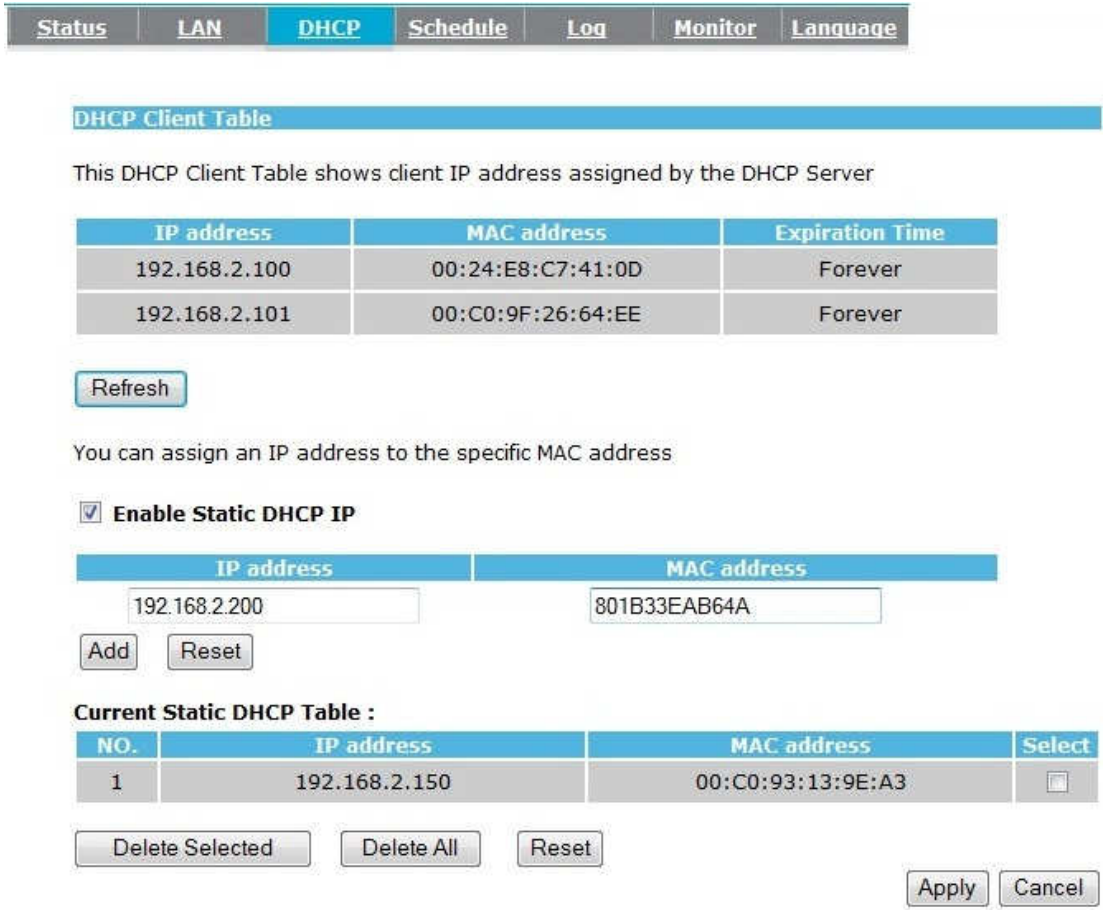


Two DNS servers can be assigned for use by your LAN devices.
There are four modes available.

DNS Servers	
From ISP	The DNS server IP address is assigned by your ISP.
User-Defined	The DNS server IP address is configured manually.
DNS Relay	When DNS Relay is enabled, the Router plays the role of a DNS server. DNS requests sent to the Router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the Router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. Do not select this option if you implement a LAN-side DNS server as a virtual server.

5.3. DHCP

This page shows the status of the DHCP server and also allows you to control how the IP addresses are allocated.



The DHCP Client Table displays a list of clients that have been allocated IP addresses from the Router's DHCP Server.

DHCP Client Table	
IP address	The LAN IP address of the client computer.
MAC address	The LAN MAC address of the client computer.
Expiration Time	The time that the allocated IP address will expire.
Refresh	Click this button to update the DHCP Client Table.

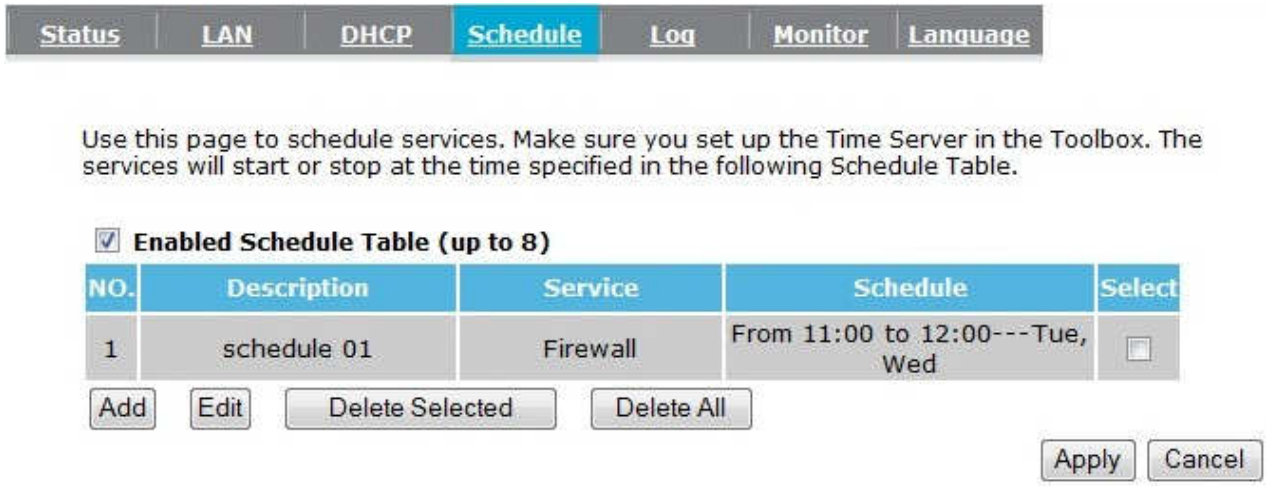
You can also manually specify the IP address that will be allocated to a LAN client by associating the IP address with its MAC address.

Enter the IP address you would like to manually assign to a specific MAC address and click **Add** to add the condition to the Static DHCP Table.

5.4. Schedule

This page allows you to schedule times that the Firewall and Power Saving features will be activated / deactivated.

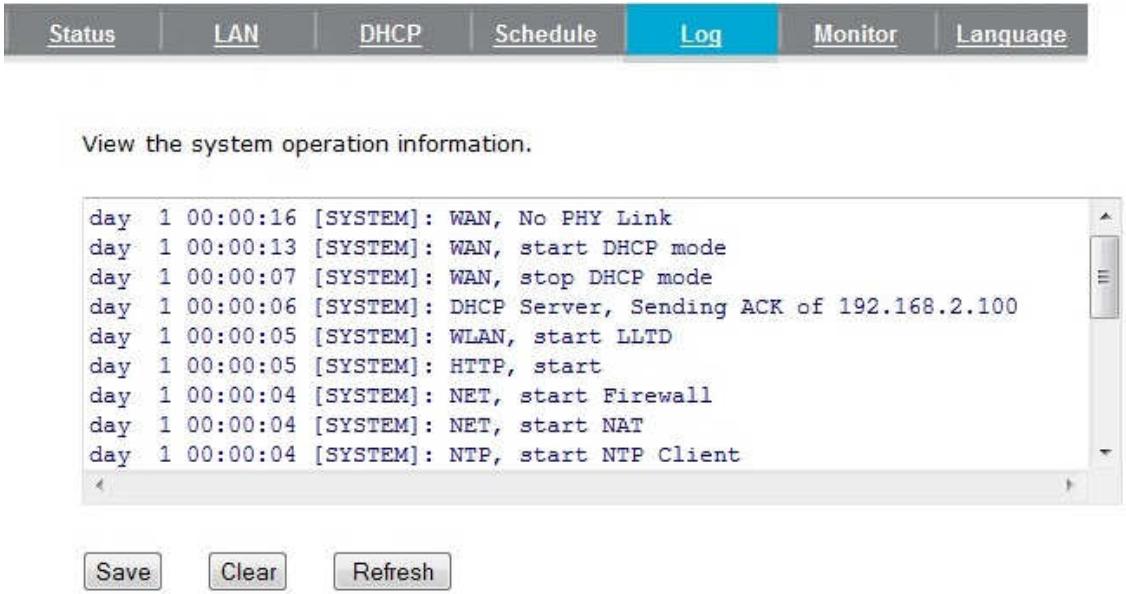
Click **Add** to create a Schedule entry.



Schedule	
Schedule Description	Assign a name to the schedule.
Service	Type of service
Days	Define the Days to activate or deactivate the scheduled service.
Time of day	Define the Time of day to activate or deactivate the scheduled service. Note: Use 24-hour clock format.

5.5. Log

This page displays the system log of the Router. When powered down or rebooted, the log will be cleared.

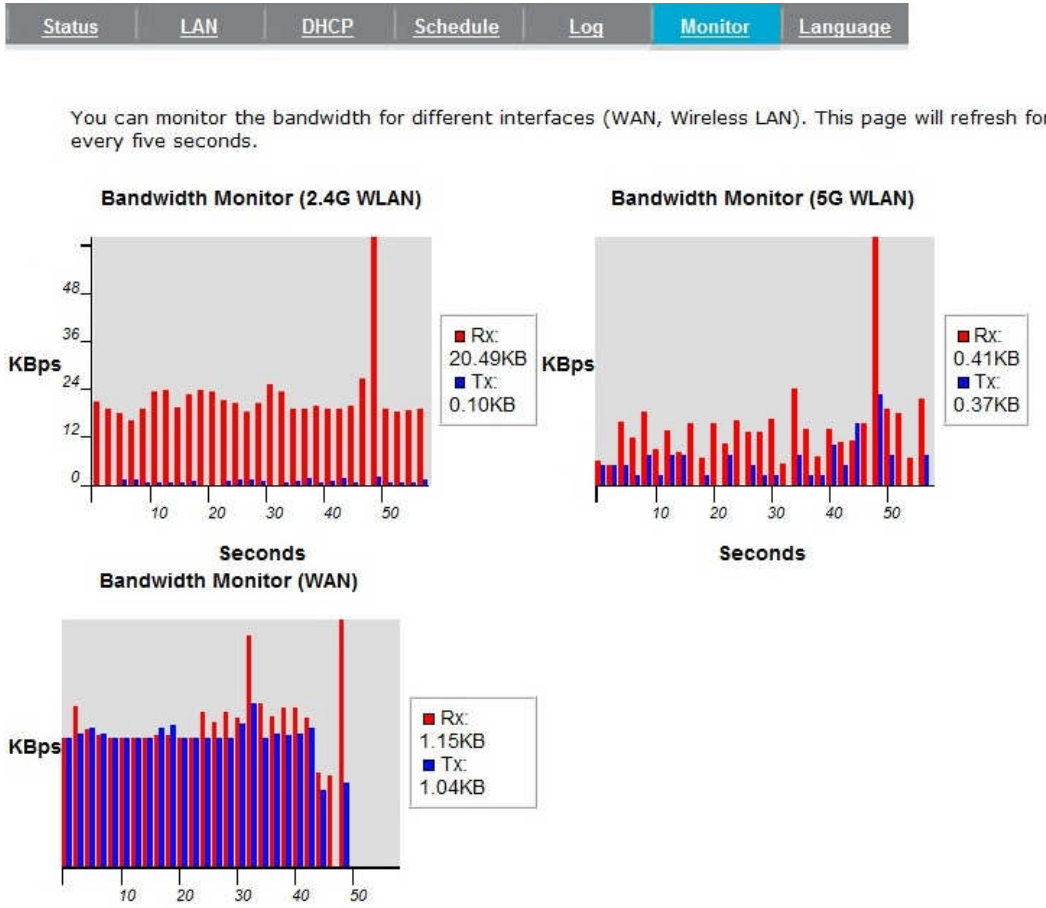


Log	
Save	Save the log to a file.
Clear	Clears the log.
Refresh	Updates the log.

5.6. Monitor

This page displays histograms of the WAN and Wireless LAN traffic.

The information is automatically updated every five seconds.



5.7. Language

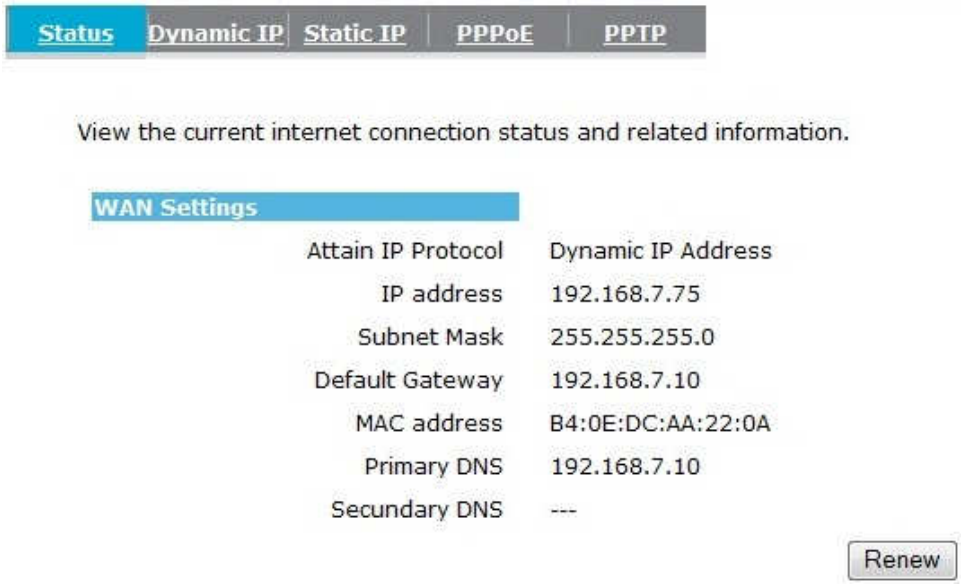
This page allows you to change the Language of the User Interface.

6. Internet

The Internet section on the left menu allows you to manually configure the WAN connection type and related settings.

6.1. Status

This page shows the current status of the Router's WAN connection.



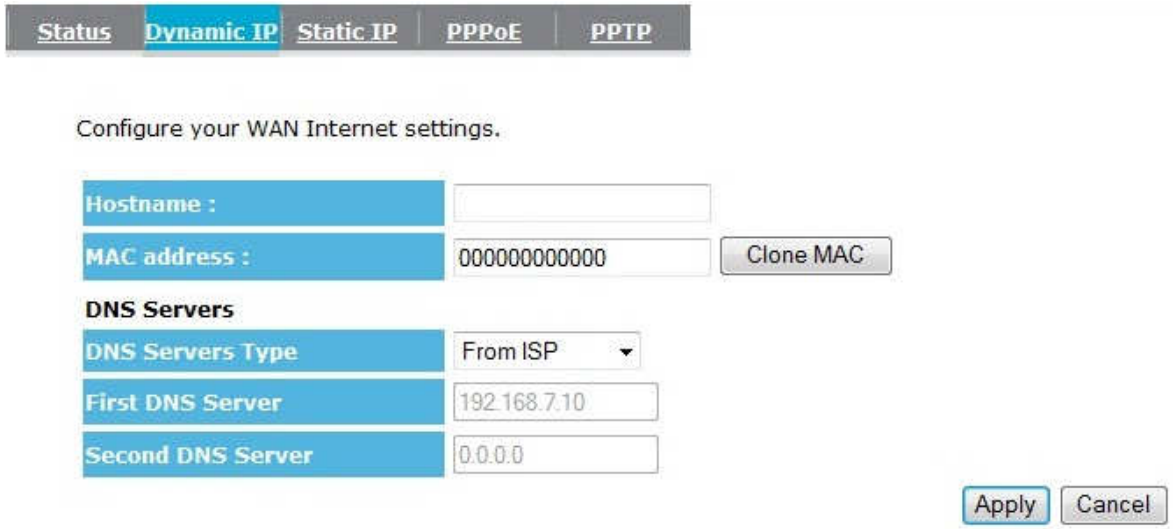
6.2. Dynamic IP Address (DHCP)

Select this option if your ISP assigns an IP address dynamically by DHCP (i.e. Cable connections).

Typically, you can leave the Hostname and MAC address fields empty.

However, some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will only accept traffic from the MAC address of that computer.

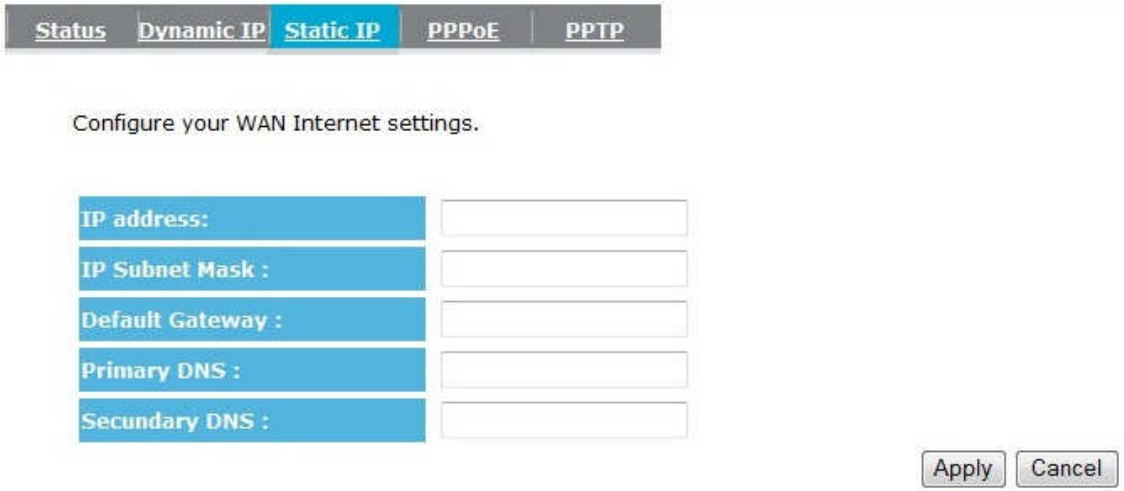
If your ISP has registered the MAC address of your computer's Ethernet LAN card, connect only the computer with the authorized MAC address and click the **Clone MAC Address** button. This function allows your router to clone the authorized MAC address of the registered computer. The correct MAC address will be used to initiate the connection to the ISP.



Dynamic IP Address	
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC Address that is used to connect to the ISP.
DNS Servers	
Two DNS servers can be assigned for use by your LAN devices. There are two modes available:	
From ISP	The DNS server's IP address is assigned by your ISP.
User-Defined	Set the DNS server's IP address manually.

6.3. Static IP Address

Select this option if your Internet Service Provider (ISP) has assigned you a permanent, fixed (static) IP address. Enter the IP address assigned by your ISP, subnet mask, default gateway IP address, and the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, also enter it here.

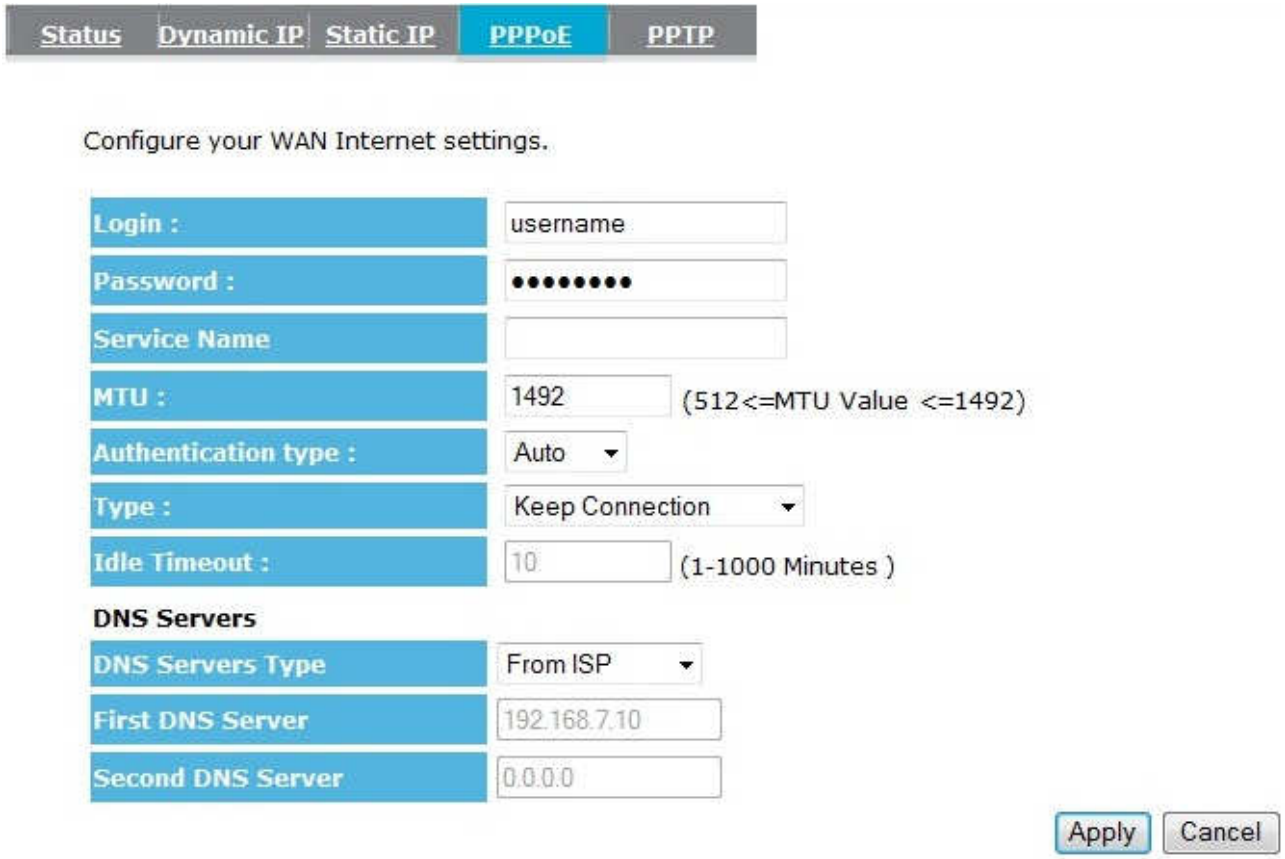


Static IP Address	
IP address	Enter the IP address assigned by your ISP.
IP Subnet Mask	Enter the subnet mask of the IP address.
Default Gateway	Enter the IP address of the default gateway.
Primary DNS	Enter the IP address of the Primary DNS server.
Secondary DNS	Enter the IP address of the Secondary DNS server (Optional).

6.4. PPP over Ethernet (PPPoE)

This protocol is used by most DSL services worldwide. Select this option if you have a DSL connection.

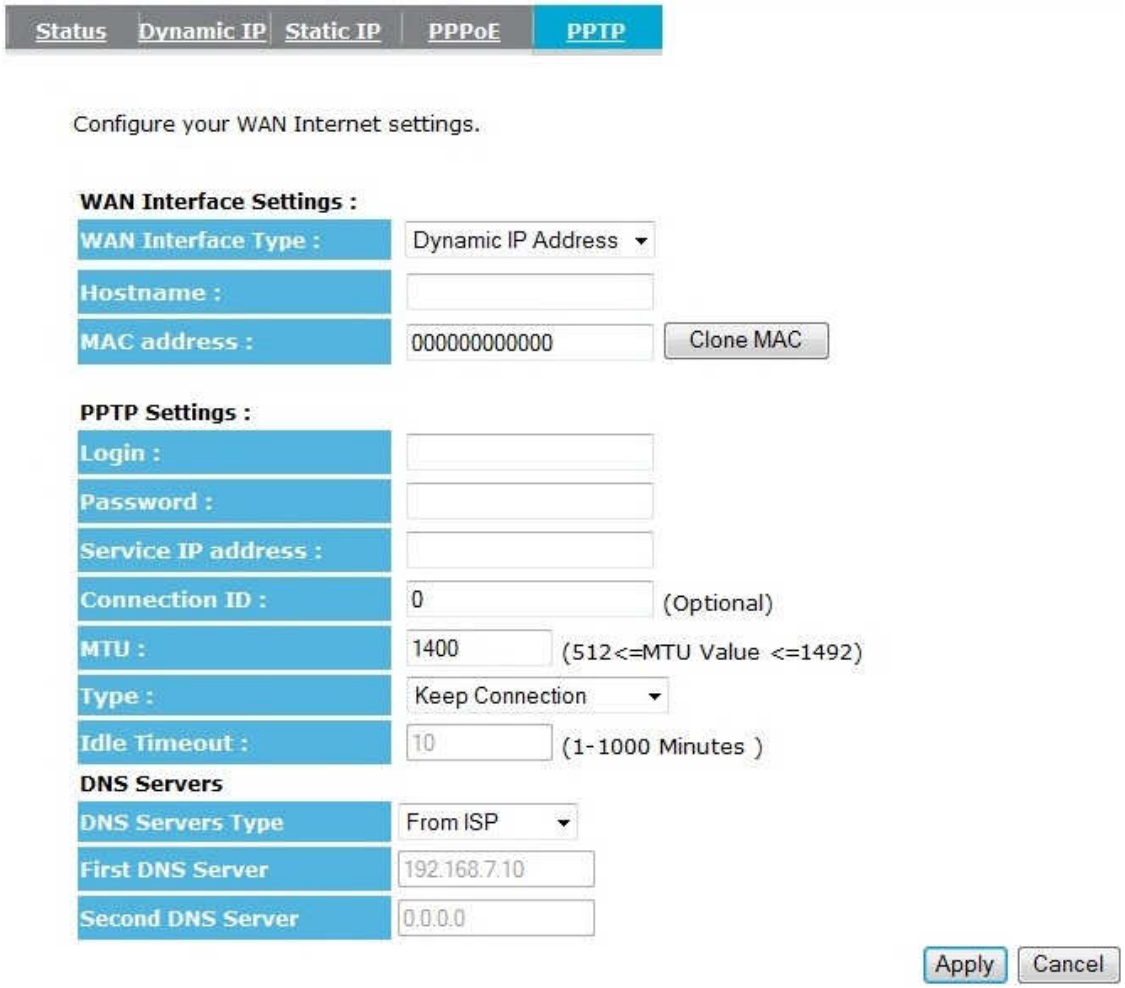
Enter the username and password provided by your ISP.



PPP over Ethernet (PPPoE)	
Username	Username assigned to you by the ISP
Password	Password for this username.
Service	You can assign a name for this service. (Optional)
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.
Authentication type	Select whether the ISP uses PAP or CHAP methods for authentication. Select **Auto** if you are not sure.
Type	You can choose the method that the router maintains connection with the ISP. **Keep Connection:** The device will maintain a constant connection with the ISP. **Automatic Connection:** The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. **Manual Connection:** The user will need to manually connect to the ISP by clicking the **Connect** button.
Idle Timeout	If the connection type is **Automatic Connection**, the Router will automatically disconnect from the ISP when there has been no Internet traffic. Note: Specify the Idle time in minutes.

6.5. Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by very few ISPs. It is used primarily in Austrian DSL services.



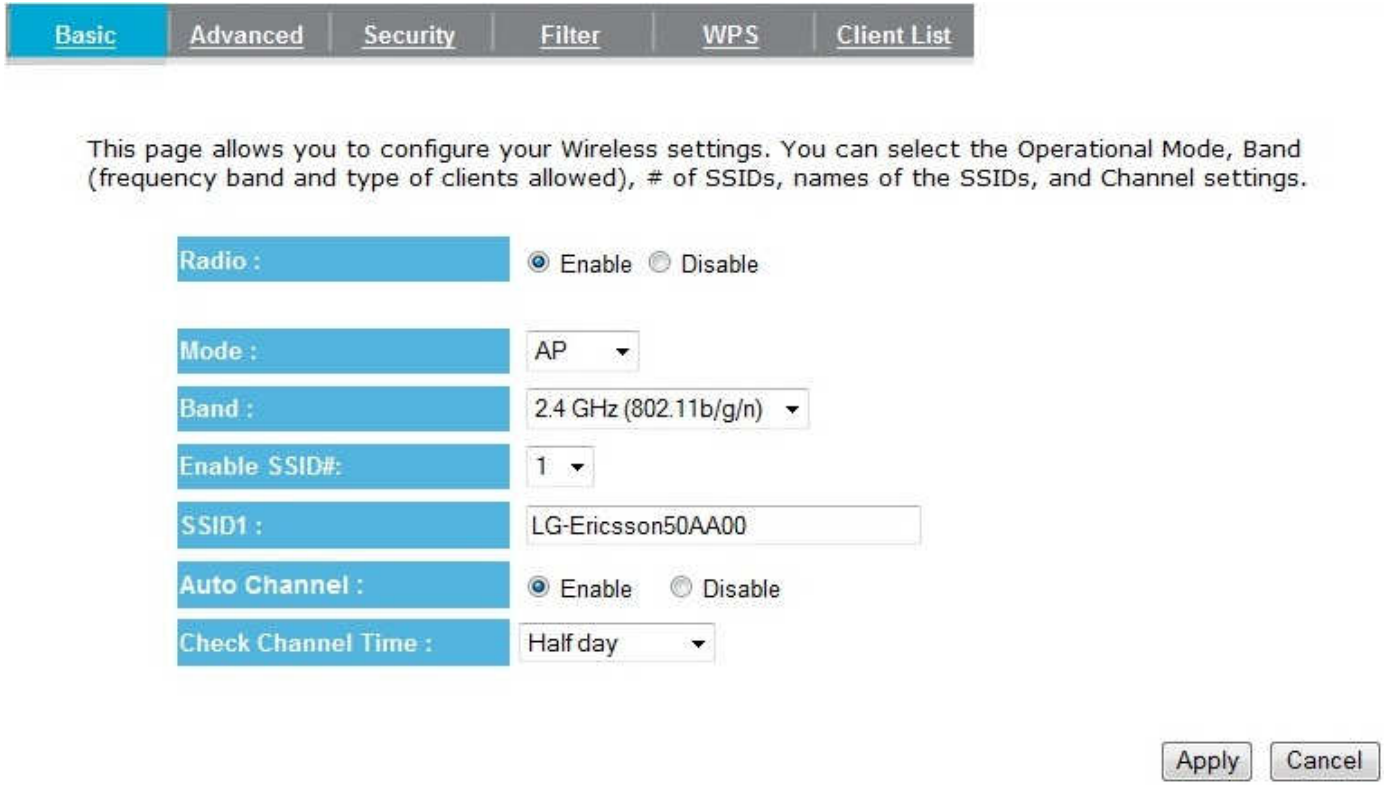
Point-to-Point Tunneling Protocol (PPTP)	
WAN Interface Type	Select whether the ISP is set to Static IP or will allocate Dynamic IP addresses.
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC Address that is used to connect to the ISP.
Login	Username assigned to you by the ISP
Password	Password for this username.
Service IP Address	The IP Address of the PPTP server.
Connection ID	This is optional. Only required if specified by ISP
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.
Type	You can choose the method that the router maintains connection with the ISP. **Keep Connection:** The device will maintain a constant connection with the ISP. **Automatic Connection:** The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. **Manual Connection:** The user will need to manually connect to the ISP by clicking the **Connect** button.
Idle Timeout	If the connection type is **Automatic Connection**, the Router will automatically disconnect from the ISP when there has been no Internet traffic. Note: Specify the Idle time in minutes.

7. Wireless 2.4G

The Wireless 2.4G section allows you to configure the wireless settings for the 2.4GHz frequency band.

7.1. Basic

The Basic page displays the current wireless settings of the Router.



Basic	
Radio	Enable or Disable wireless.
Mode	Select from Access Point (AP) or Wireless Distribution System (WDS) modes. (Default: AP)
Band	Select the types of wireless clients that the device will accept. Example: **2.4 GHz (b/g/n):** All 802.11b/g/n clients will be allowed. **2.4 GHz (b/g)**: Only 802.11b/g clients will be allowed. **2.4 GHz (n)**: Only 802.11n clients will be allowed.
Enable SSID#	Select the number of SSIDs (Wireless Networks) you would like to enable. You can create up to 4 separate wireless networks by enabling 4 SSIDs.
SSID#	Enter the name of your wireless network. You can use up to 32 characters. Example: “Life Is Good”, “Guest Network”, etc.
Auto Channel	When Enabled, the Router will scan the wireless signals around your area and select the channel with the least interference. When Disabled, you will need to configure the Channel settings on the Router.
Channel	Manually select which channel the wireless signal will use.
Check Channel Time	When Auto Channel is Enabled, you can specify the frequency the Router will scan the wireless signals around your area.

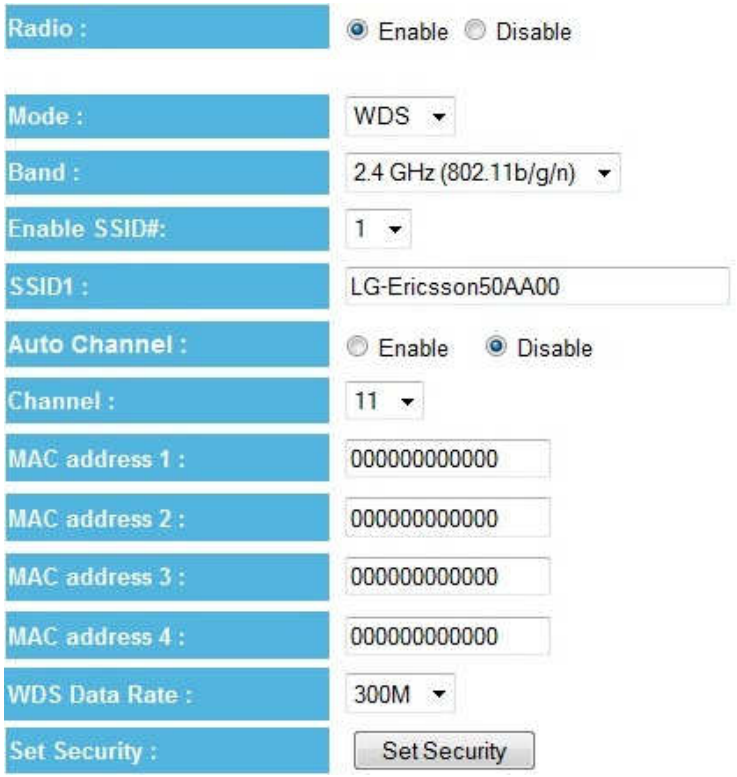
Wireless Distribution System (WDS)

When WDS is enabled, the Router functions as a wireless repeater and is able to wireless communicate with other APs via WDS links. WDS allows you to connect Access Points wirelessly and extend a wired infrastructure to locations where cabling is impossible or difficult to implement.

To create a WDS network, enter the MAC addresses of the Access Points that you want included in the WDS links. There can be a maximum of four access points.

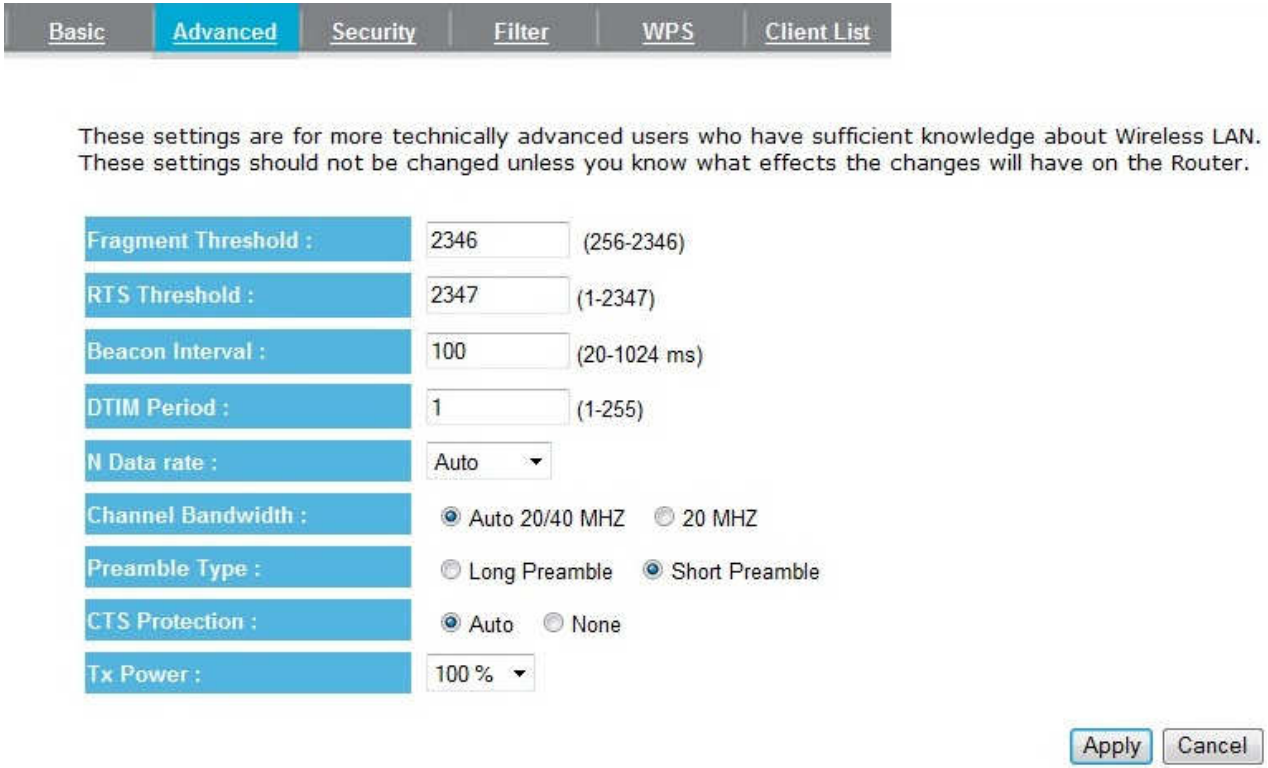
Important:

- A WDS link is bidirectional; so this AP must know the MAC Address of the other AP, and the other AP must also have a WDS link back to this AP. **Make sure the APs are configured with the same Channel and Security settings**.
- Compatibility between different brands and models is not guaranteed. It is recommended that the WDS network be created using products from the same manufacturer for maximum compatibility.



7.2. Advanced

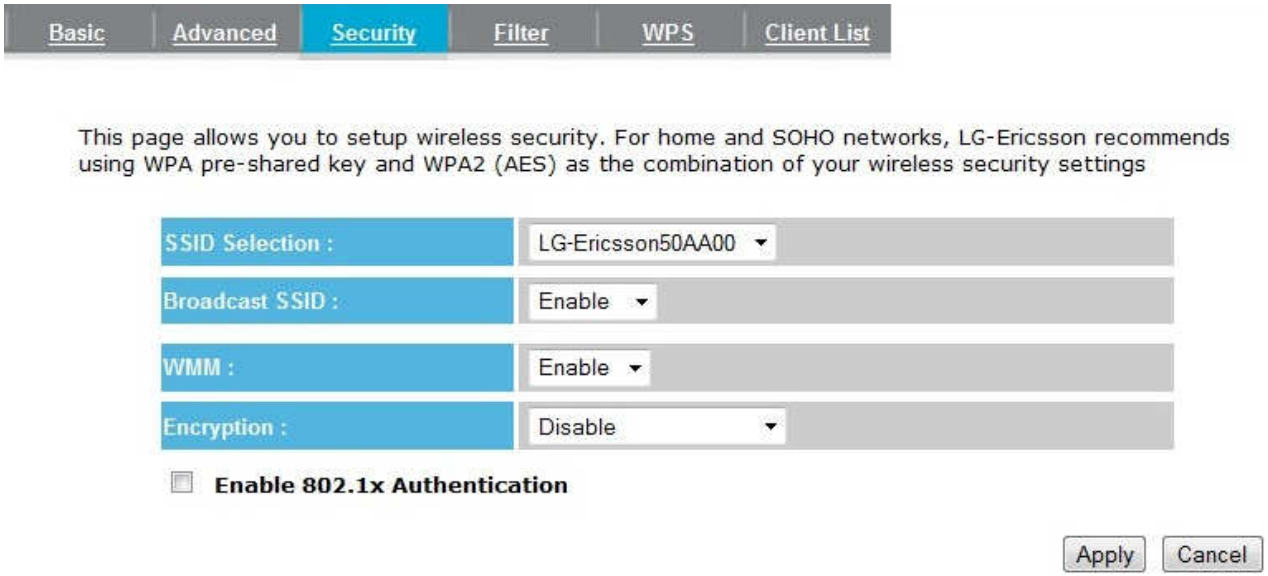
This page allows you to configure advanced wireless settings. It is recommended that default settings are used unless you have experience with these advanced functions.



Advanced	
Fragment Threshold	Specifies the size of the packet per fragment. Selecting a smaller number can reduce the chance of packet collision. However, when the value is set too low, increased overhead will likely result in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, the packet will be sent without RTS/CTS handshake which may result in incorrect transmission.
Beacon Interval	The time interval that the device broadcasts a beacon. This beacon is used to synchronize all wireless clients on the network.
DTIM Period	A Delivery Traffic Indication Message informs all wireless clients that the access point will be sending Multicast data.
N Data Rate	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
Channel Bandwidth	Set whether each channel uses 20 or 40Mhz. To achieve maximum 802.11n speeds, 40Mhz channels must be used.
Preamble Type	A preamble is a message that helps access points synchronize with the client. **Long Preamble** is standard-based so it increases compatibility. **Short Preamble** is not standard-based so it decreases compatibility; however it also increases performance. Auto as default.
CTS Protection	When Enabled, the performance is slightly lower however the chances of packet collision is greatly reduced.
Tx Power	Set the power output of the wireless signal.

7.3. Security

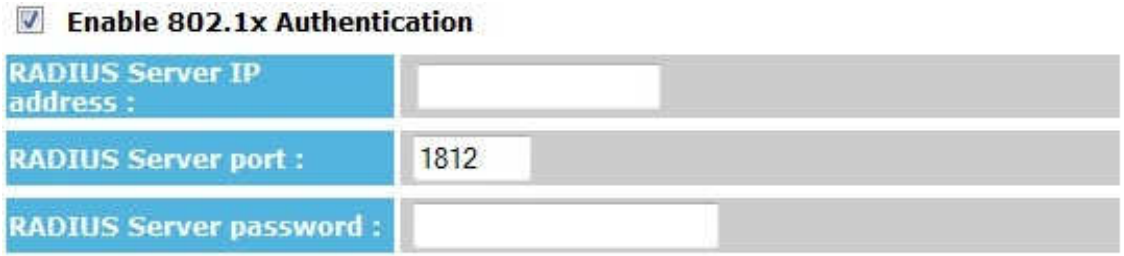
This page allows you to configure the wireless security settings. Select the SSID to which you want to apply the security settings, and select your preferred security type from the Encryption drop-down list. We recommend choosing **WPA-PSK** as the Encryption type and **WPA2 (AES)** as the WPA type for your home network. Enter a passphrase (security key) for your wireless network and click **Apply**.



Security	
SSID Selection	Select the SSID to apply the security settings.
Broadcast SSID	If Disabled, the Router will not broadcast the SSID. The SSID will be invisible to wireless clients.

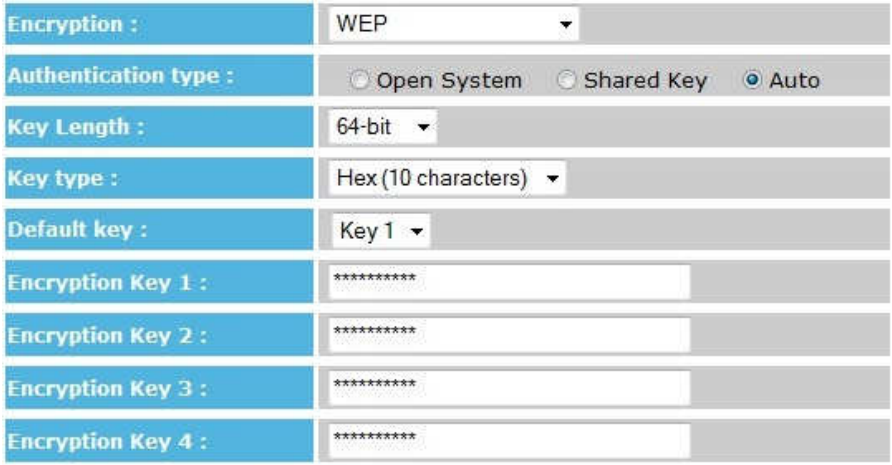
WMM	Wi-Fi Multi-Media is a Quality of Service (QoS) protocol which prioritizes traffic in the order according to voice, video, best effort, and background. Note: In certain situations, WMM needs to be enabled to achieve 11n transfer speeds.
Encryption	The encryption method to be applied. You can choose from WEP, WPA pre-shared key or WPA RADIUS. • **Disabled** - no data encryption is used. LG-Ericsson strongly recommends that you set up wireless security. • **WEP** - data is encrypted using the WEP standard. • **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP. • **WPA2-PSK** - This is a further development of WPA-PSK and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption. • **WPA-RADIUS** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard. If this option is selected: • This Access Point must have a "client login" on the Radius Server. • Each user must have a "user login" on the Radius Server. • Each user's wireless client must support 802.1x and provide the login data when required. • All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.



802.1x Authentication	
RADIUS Server IP Address	The IP Address of the RADIUS Server.
RADIUS Server port	The port number of the RADIUS Server.
RADIUS Server password	The RADIUS Server's password.

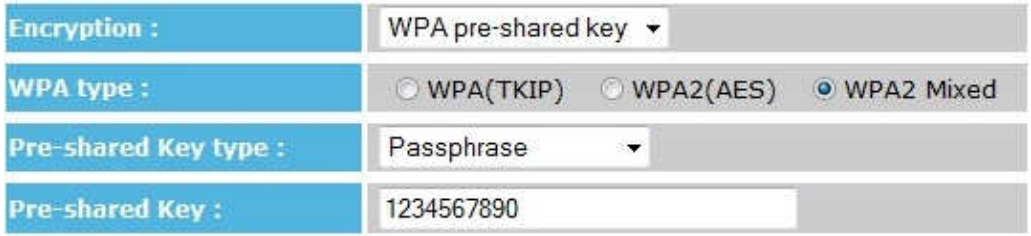
WEP Encryption:



WEP Encryption	
Authentication Type	Please ensure that your wireless clients use the same authentication type.
Key type	ASCII: Regular text (recommended) HEX: For advanced users (uses 0~9 and A~F)
Key Length	Select the desired option, and ensure the wireless clients use the same setting. • **64-bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64-bit Encryption, the key size is 10 characters in HEX (0~9 and A~F). • **128-bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128-bit Encryption, the key size is 26 characters in HEX (0~9 and A~F).
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a **Key Value** for the **Default Key**.

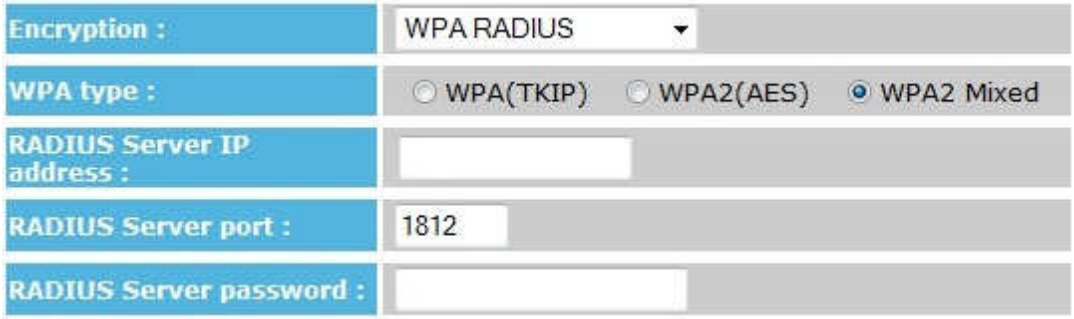
Encryption Key #	Enter the key value or values you wish to use. Only the Key selected as Default is required. The others are optional.

WPA Pre-Shared Key Encryption:



WPA Pre-Shared Key Encryption	
Authentication Type	Please ensure that your wireless clients use the same authentication type.
WPA type	Select the preferred WPA encryption type. The recommended WPA type is **WPA2 (AES)**. Make sure your wireless clients use the same settings.
Pre-shared Key Type	Select whether you would like to enter the Key in Passphrase or HEX format. Default: **Passphrase** (you can use any character from 0~9 and A~Z, with a length from **8 to 63** characters)
Pre-shared Key:	This is the key or password to the wireless network. Wireless clients must use the same key to connect. Note: If using the Passphrase format, the key must be from **8 to 63** characters in length.

WPA RADIUS Encryption:



WPA RADIUS Encryption	
WPA type	Select the preferred WPA encryption type. Make sure your wireless clients use the same settings.
RADIUS Server IP address	Enter the IP address of the RADIUS Server.
RADIUS Server Port	Enter the port number used for connecting to the RADIUS server.
RADIUS Server password	Enter the password required to connect to the RADIUS server.

7.4. Filter

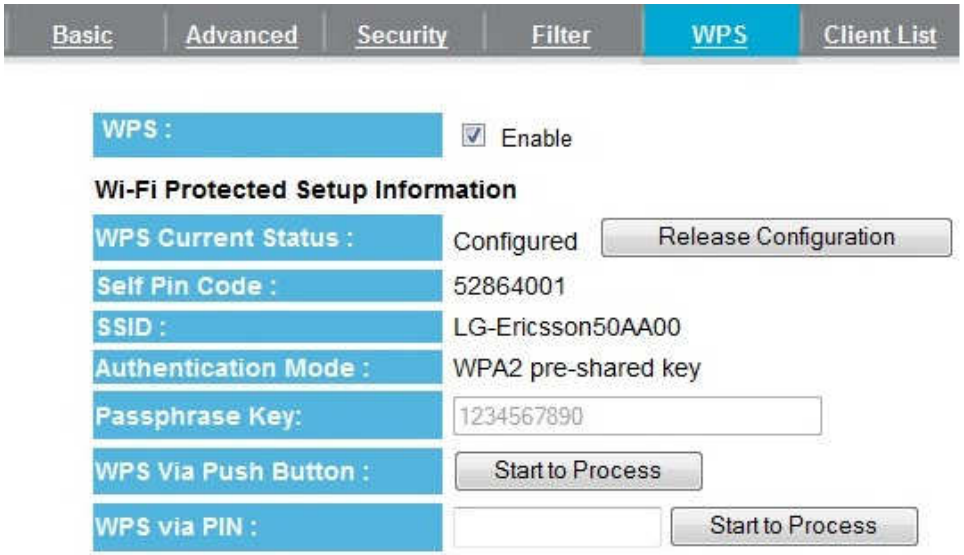
This page allows you to create filters to control which wireless clients can connect to the Router. When Wireless Access Control is enabled, only wireless clients with the MAC addresses entered into the Filtering Table are allowed to connect.

Wireless Filter	
Enable Wireless Access Control	Check the box to enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
Description	Enter a name or description for this entry.
MAC address	Enter the MAC address of the wireless client allowed.
Add	Click this button to add the entry.
Reset	Click this button to reset the MAC address and Description fields.
MAC Address Filtering Table	
Only clients listed in this table will be allowed to connect to the wireless network.	
Delete Selected	Delete the selected entries.
Delete All	Delete all entries.
Reset	Un-check all selected entries.

7.5. Wi-Fi Protected Setup (WPS)

The WPS feature is based on the Wi-Fi Alliance WPS standard. The goal is to simplify the set up of security-enabled wireless networks in the home and small office environments.

The WPS function simplifies the steps required to connect to a secured wireless network. Two WPS methods are supported: **WPA via Push Button (PBC)** and **WPS via PIN (PIN)**.



Wi-Fi Protected Setup (WPS)	
WPS	Check the box to enable the WPS feature.
WPS Button	Check to Enable the WPS push button.
Wi-Fi Protected Setup Information	
WPS Current Status	Shows whether the WPS function is **Configured** or **Unconfigured**. Configured means that WPS has been used to authorize connection between the device and wireless clients.
SSID	The SSID (name of the wireless network) used when connecting using WPS.
Authentication Mode	The encryption method used by the WPS process.
Passphrase Key	This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempt to connect to the wireless network.
WPS Via Push Button	Click this button to initialize the WPS feature using the push button method.
WPS Via PIN	Enter the PIN code from wireless adapter and then click [**Start to Process**] button to initialize the WPS feature.

There are two methods to initialize the WPS feature: **WPS via Push Button (PBC)** and **WPS via Pin (PIN)**.

1. **Push Button Method (PBC – Push Button Connect)**

   Press the WPS button on your wireless adapter and press the WPS button on the top panel of the Router to establish the connection.

   – Or –

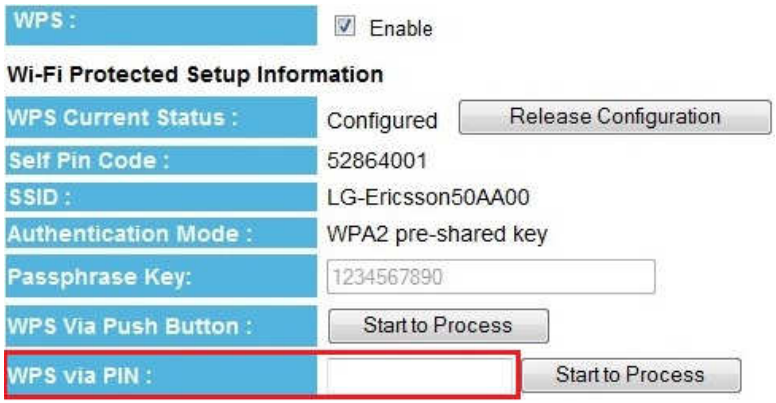
   a. Log into the browser utility of the Router (see "Manually enter Setup Wizard" in section 4).

   b. Click the **Wireless** tab on the left menu, and then click the **WPS** tab on the top menu.

   c. Next to "WPS Via Push Button", click **Start to Process** to establish the connection.

2. **Pin Code Method (PIN)**

   Enter the PIN code of wireless adapter in WPS Via PIN field and then click [**Start to Process**] button to initialize the WPS process. Note that this process may be different for each brand/model. Refer to the user manual of your wireless client adapter for more information.



7.6. Client List

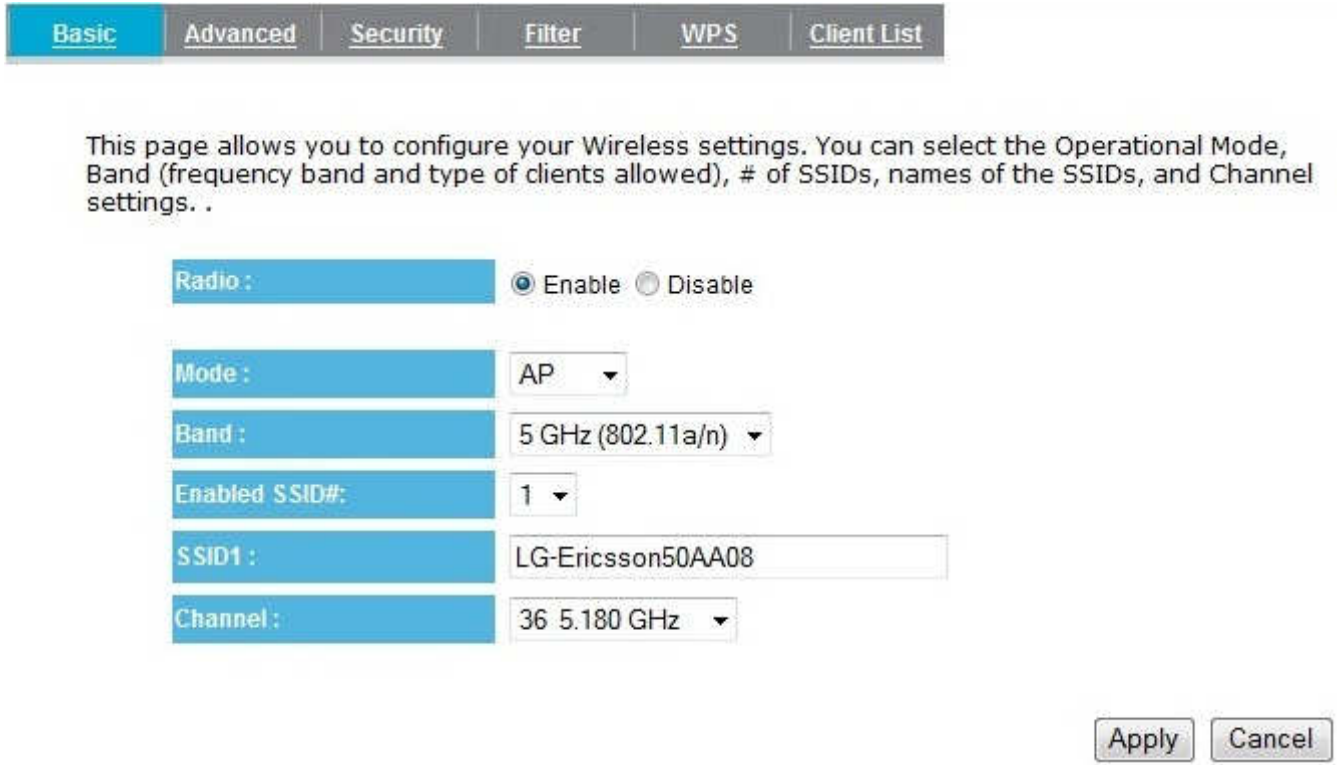
This page shows the wireless clients that are connected to the Router.

8. Wireless 5G

The Wireless section allows you to configure the wireless settings for the 5GHz frequency band.

8.1. Basic

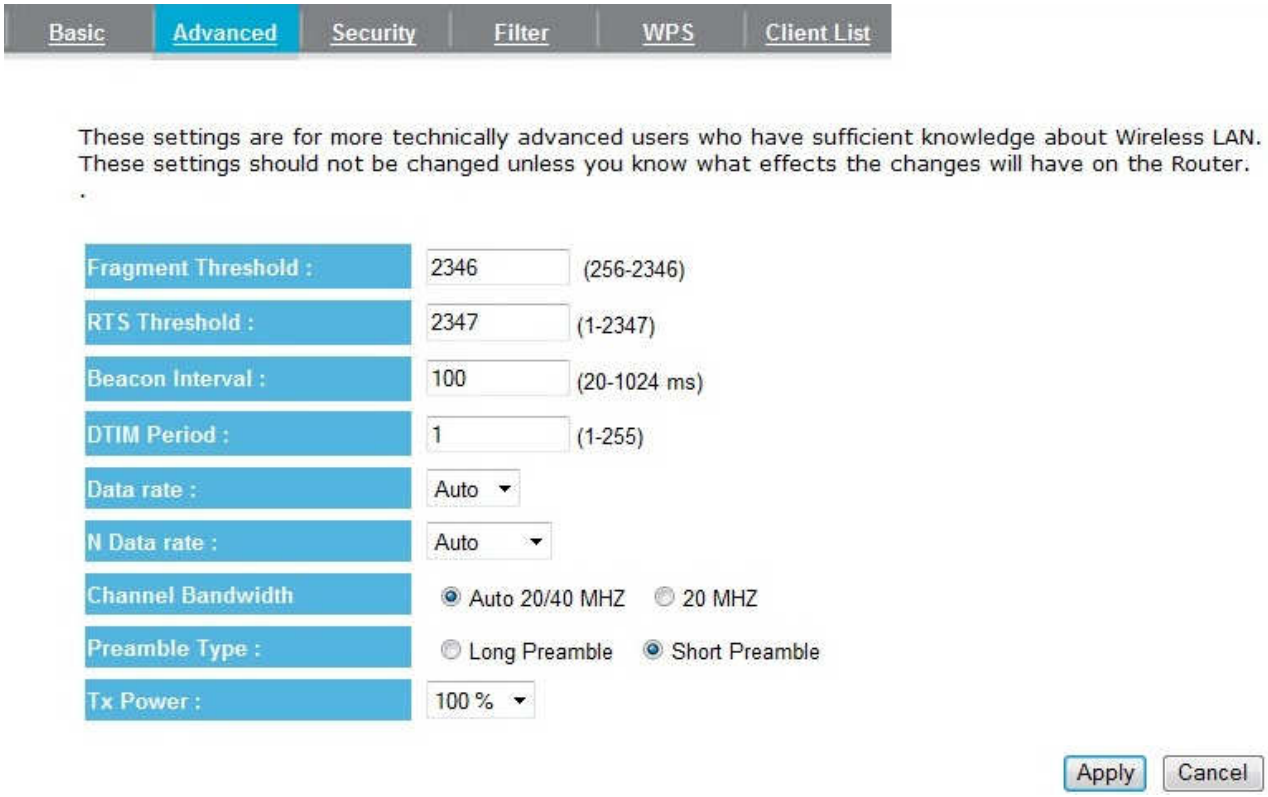
The Basic page displays the current wireless settings of the Router. For WDS setting, please refer to **section 7.1**.



Basic	
Radio	Enable or Disable wireless.
Mode	Select from Access Point (AP) or Wireless Distribution System (WDS) modes. (Default: AP)
Band	Select the types of wireless clients that the device will accept. Example: **5 GHz (a/n):** All 802.11a/n clients will be allowed. **5 GHz (a)**: Only 802.11a clients will be allowed. **5 GHz (n)**: Only 802.11n clients will be allowed.
Enable SSID#	Select the number of SSIDs (Wireless Networks) you would like to enable. You can create up to 4 separate wireless networks by enabling 4 SSIDs.
SSID#	Enter the name of your wireless network. You can use up to 32 characters. Example: “Life Is Good”, “Guest Network”, etc.
Channel	Manually select which channel the wireless signal will use.

8.2. Advanced

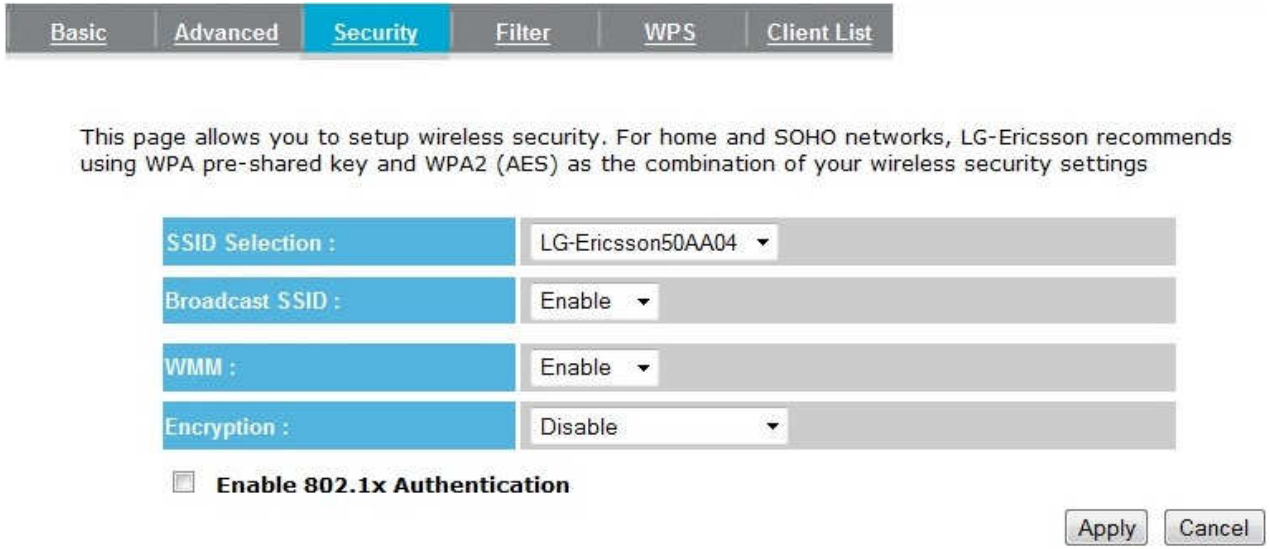
This page allows you to configure advanced wireless settings. It is recommended that default settings are used unless you have experience with these advanced functions.



Advanced	
Fragment Threshold	Specifies the size of the packet per fragment. Selecting a smaller number can reduce the chance of packet collision. However, when the value is set too low, increased overhead will likely result in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, the packet will be sent without RTS/CTS handshake which may result in incorrect transmission.
Beacon Interval	The time interval that the device broadcasts a beacon. This beacon is used to synchronize all wireless clients on the network.
DTIM Period	A Delivery Traffic Indication Message informs all wireless clients that the access point will be sending Multicast data.
N Data Rate	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
Channel Bandwidth	Set whether each channel uses 20 or 40Mhz. To achieve maximum 802.11n speeds, 40Mhz channels must be used.
Preamble Type	A preamble is a message that helps access points synchronize with the client. **Long Preamble** is standard-based so it increases compatibility. **Short Preamble** is not standard-based so it decreases compatibility; however it also increases performance. Auto as default.
Tx Power	Set the power output of the wireless signal.

8.3. Security

This page allows you to configure the wireless security settings. For more details, please refer to **section 7.3**.



8.4. Filter

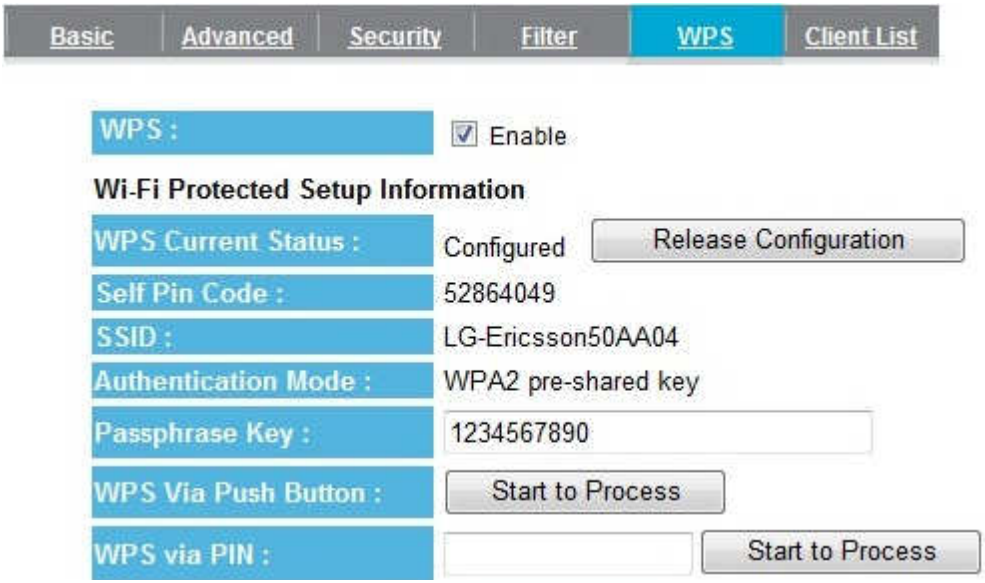
This page allows you to create filters to control which wireless clients can connect to the Router. When Wireless Access Control is enabled, only wireless clients with the MAC addresses entered into the Filtering Table are allowed to connect.

Wireless Filter	
Enable Wireless Access Control	Check the box to enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
Description	Enter a name or description for this entry.
MAC address	Enter the MAC address of the wireless client allowed.
Add	Click this button to add the entry.
Reset	Click this button to reset the MAC address and Description fields.
MAC Address Filtering Table	
Only clients listed in this table will be allowed to connect to the wireless network.	
Delete Selected	Delete the selected entries.
Delete All	Delete all entries.
Reset	Un-check all selected entries.

8.5. Wi-Fi Protected Setup (WPS)

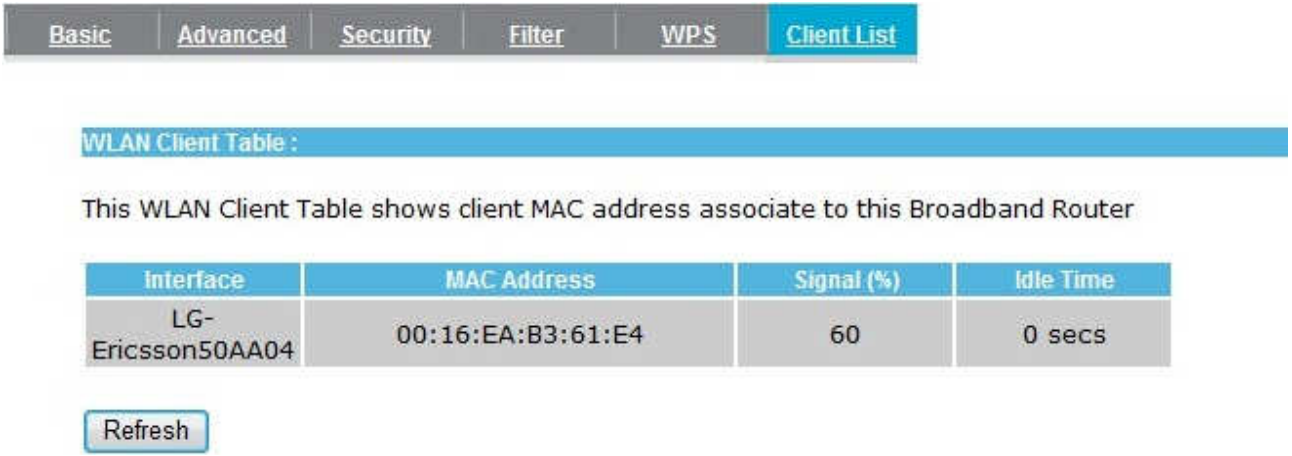
The WPS feature is based on the Wi-Fi Alliance WPS standard. The goal is to simplify the set up of security-enabled wireless networks in the home and small office environments.

The WPS function simplifies the steps required to connect to a secured wireless network. Two WPS methods are supported: **WPA via Push Button (PBC)** and **WPS via PIN (PIN)**. For more details, please refer to **section 7.5**.



8.6. Client List

This page shows the wireless clients that are connected to the Router.



9. Firewall

The Firewall section allows you to configure Firewall and Access Control settings.

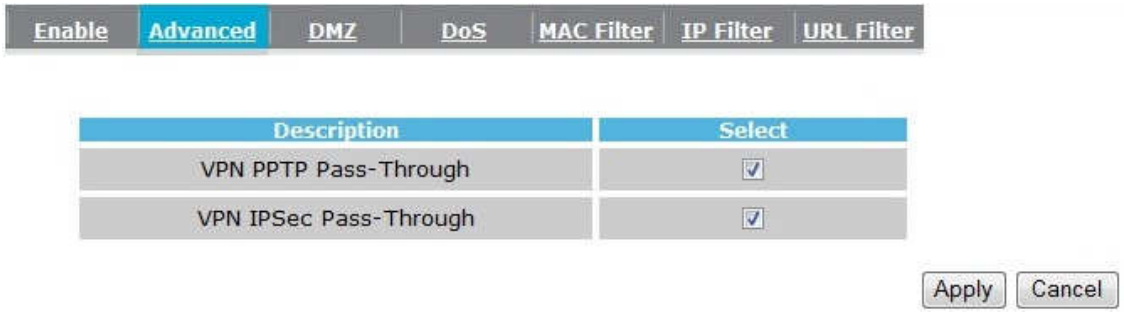
9.1. Enable

This page allows you to Enable / Disable the Firewall features.

When Firewall is enabled, Denial of Service (DoS) and SPI (Stateful Packet Inspection) features are also enabled.

9.2. Advanced

You can choose whether to allow VPN (Virtual Private Network) packets to pass through the Firewall.



9.3. DMZ (Demilitarized Zone)

If you are operating a web server, a mail server, or a web camera, you may want to expose that device to the Internet so anybody can access it. When the DMZ function is enabled, the DMZ computer is exposed to all users on the Internet. It can be accessed by both users on the Internet as well as users in the Local Network.

This feature is normally not used as it presents significant security risks to the device that you designate for the DMZ. The DMZ device is not protected by the built-in firewalls, Internet filters, or router web filters, and is open to attacks from hackers. The "DMZ PC" will receive all unknown connections and data.

If the DMZ feature is enabled, enter the IP address of the PC to be used as the "DMZ PC". You should first configure this device with a static IP address.

Note: For security reasons, you should only enable the DMZ feature when required.

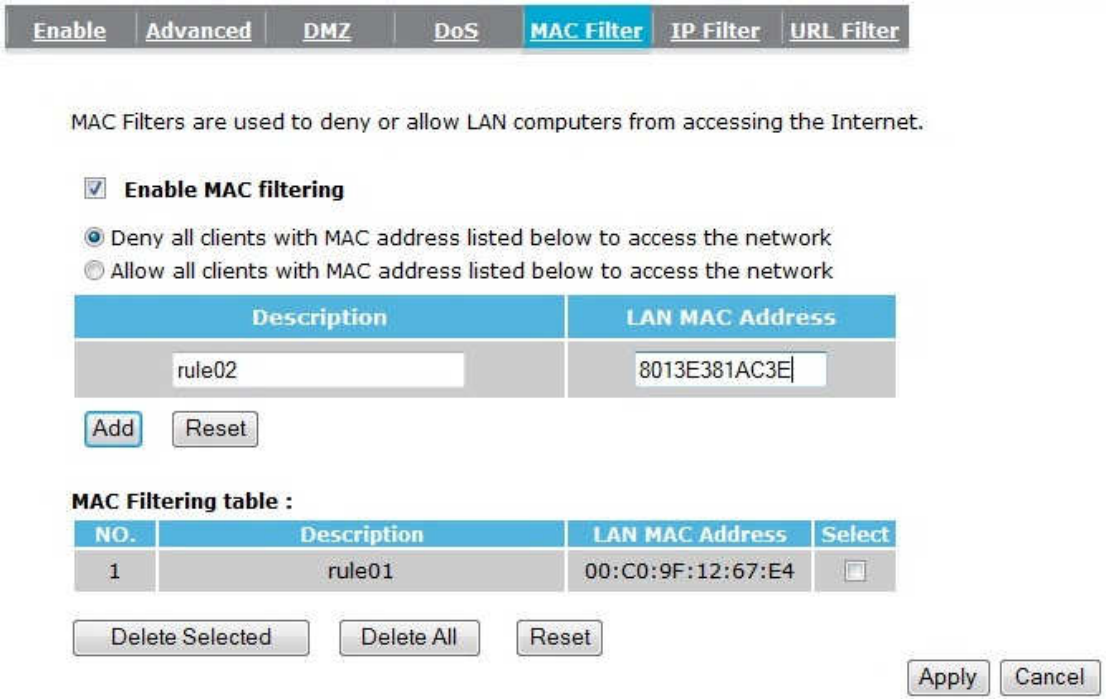
9.4. Denial of Service (DoS)

Denial of Service (DoS) is a type of Internet attack that sends a high amount of data to you with the intent to overload your Internet connection.

Enable the DoS firewall feature to automatically detect and block these DoS attacks.

9.5. MAC Filter

You can choose whether to Deny or Allow only those devices listed in the MAC Filtering table to access the Internet.

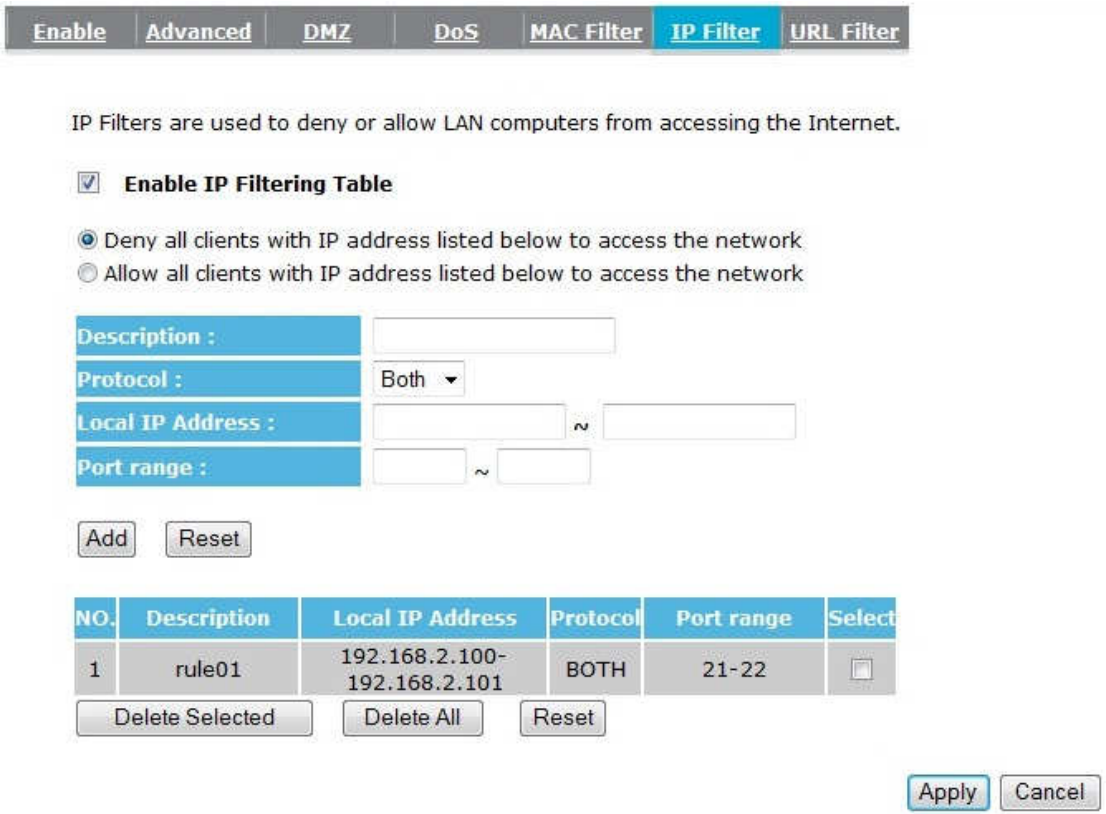


MAC Filter	
Enable MAC filtering	Check this box to enable the MAC filtering feature.
Deny all clients with MAC addresses listed below to access the network	When selected, the computers listed in the MAC Filtering table will be **Denied** to access the Internet.
Allow all clients with MAC addresses listed below to access the network	When selected, only the computers listed in the MAC Filtering table will be **Allowed** to access the Internet.

9.6. IP Filter

You can choose whether to Deny or Allow only devices with those IP Addresses listed on the IP Filtering Table from accessing certain ports.

This can be used to control which Internet applications the computers can access.
Note - You will need to have knowledge of what Internet port numbers each application uses.

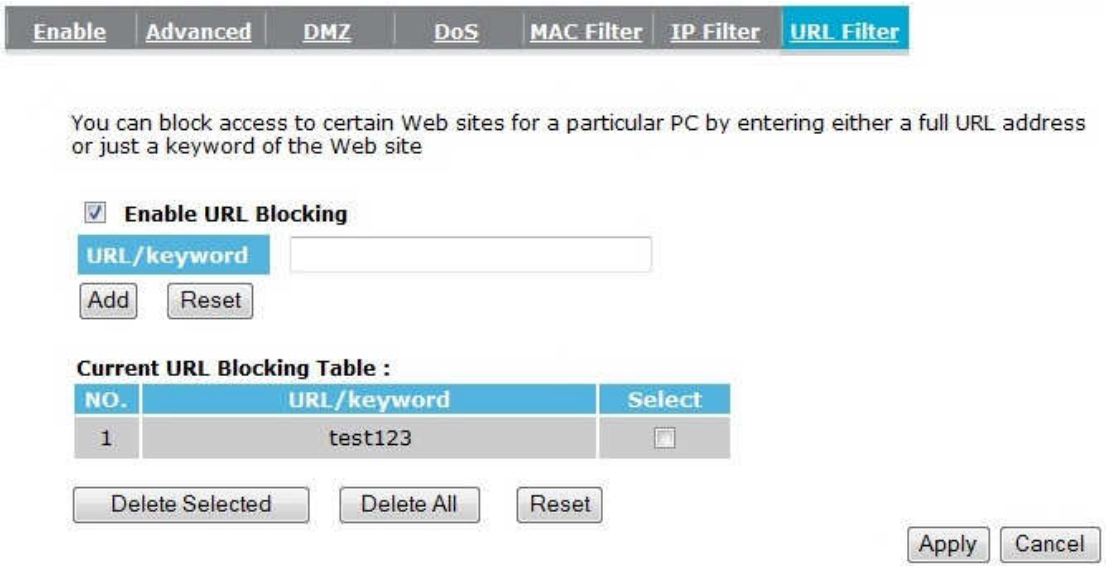


IP Filter	
Enable IP filtering	Check this box to enable the IP filtering feature.
Deny all clients with IP addresses listed below to access the network	When selected, the computers with IP addresses specified on the table will be **Denied** access to the indicated Internet port range.
Allow all clients with IP addresses listed below to access the network	When selected, the computers with IP addresses specified on the table will be **Allowed** access only to the indicated Internet port range.

9.7. URL Filter

You can deny access to certain websites by blocking keywords in the URL web address.

For example, “test123” has been added to the URL Blocking Table. Any web address that includes “test123” will be blocked.



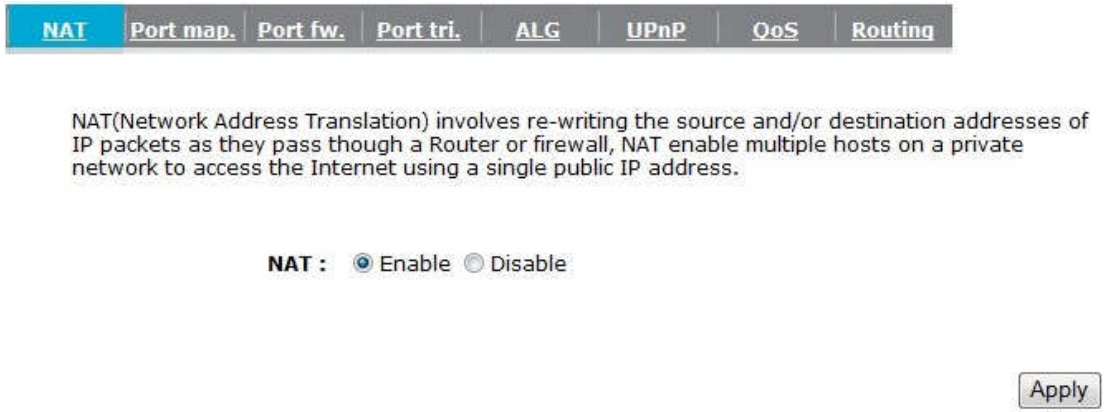
10. Advanced

The Advanced section allows you to configure the **Advanced** settings of the Router.

10.1. Network Address Translation (NAT)

This page allows you to Enable / Disable the Network Address Translation (NAT) feature. The NAT feature is required to share one Internet account with multiple LAN users.

It also is required for certain Firewall features to work properly.

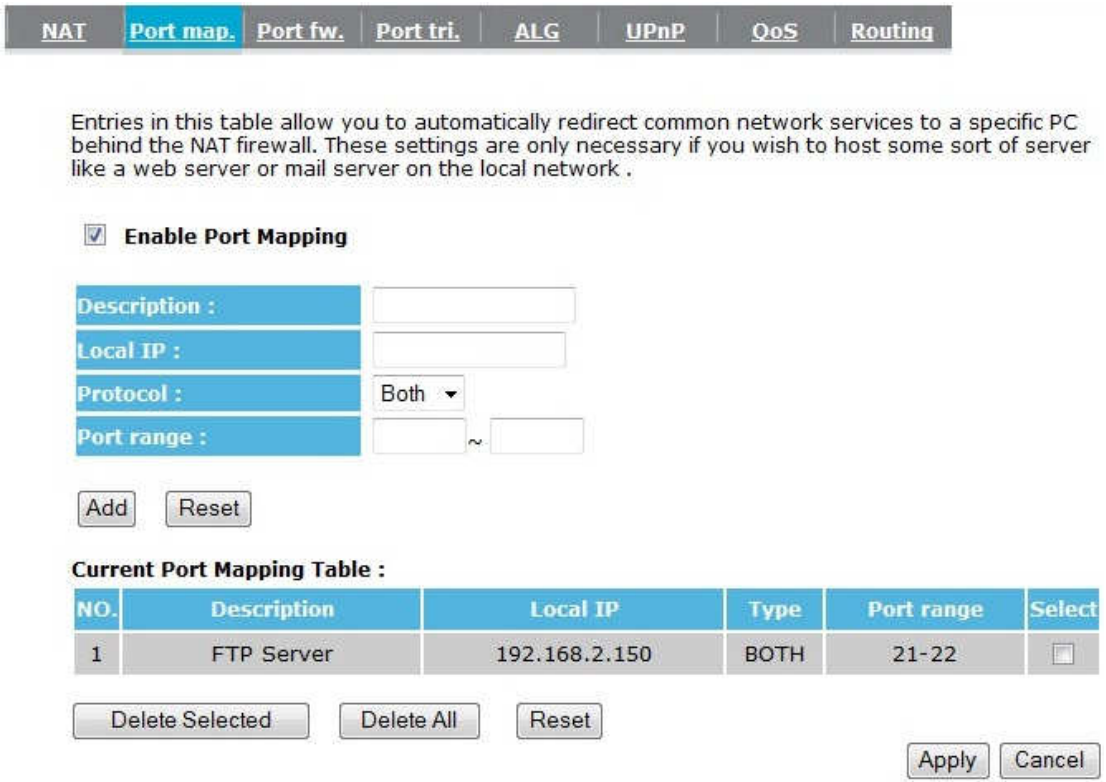


10.2. Port Mapping

Port Mapping allows you to redirect a particular range of ports to a computer on your LAN network. This helps you host servers behind the NAT and Firewall.

In the example below, there is a FTP Server that requires ports 21 to 22.

When there is a connection from the Internet on those ports, it will be redirected to the FTP Server at IP address 192.168.2.150.



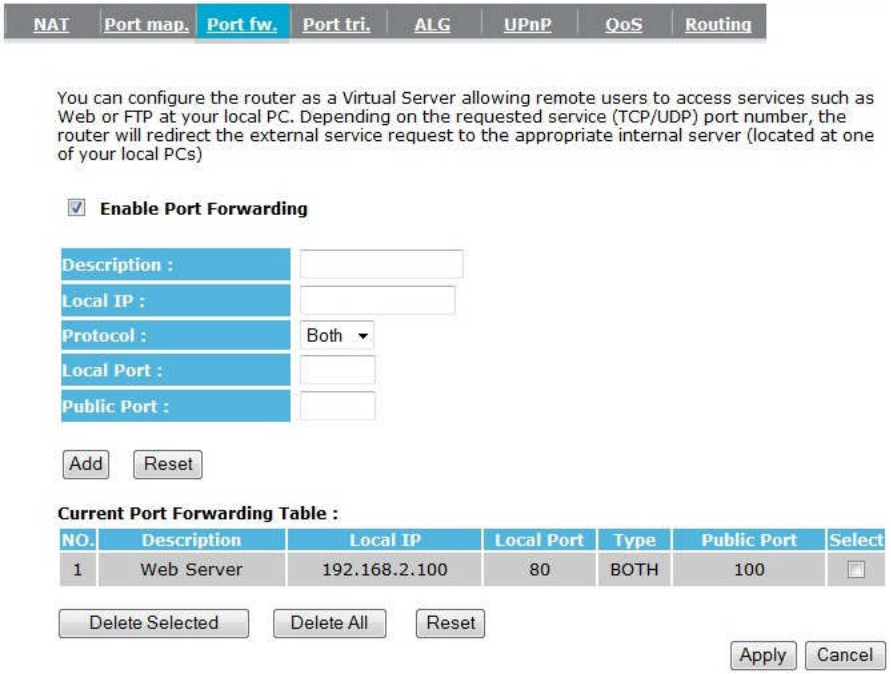
Port Mapping	
Enable Port Mapping	Check this box to enable the Port Mapping feature.
Description	Enter a name or description for this entry.
Local IP	The local IP address of the computer the server is hosted on.
Protocol	Select to apply the feature to TCP, UDP or Both types of packet transmissions.
Port range	The range of ports that this feature will be applied to.

10.3. Port Forwarding

Port Forwarding allows you to redirect a particular public port to a computer on your LAN network. This helps you host servers behind the NAT and Firewall.

In the example below, there is a Web Server running on port 80 on the LAN.
For security reasons, the Administrator would like to provide this server to Internet connection on port 100.

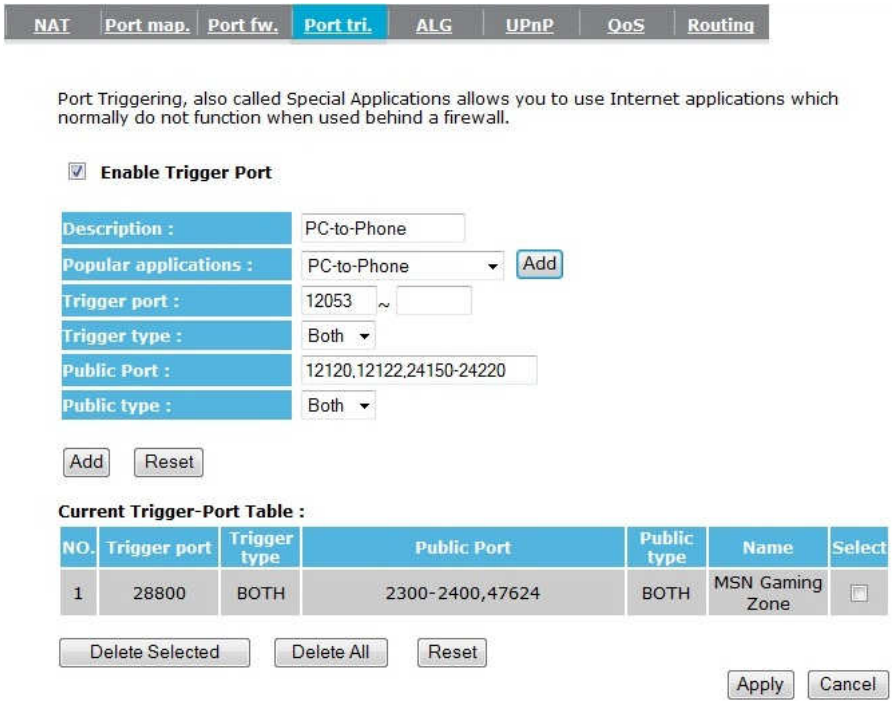
Therefore when there is a connection from the Internet on port 100, it will be forwarded to the computer with the IP address 192.168.2.100 and changed to port 80.



Port Forwarding	
Enable Port Forwarding	Check this box to enable the Port Forwarding feature.
Description	Enter a name or description for this entry.
Local IP	The local IP address of the computer the server is hosted on.
Protocol	Select to apply the feature to TCP, UDP or Both types of packet transmissions.
Local Port	The port that the server is running on the local computer.
Public Port	When a connection from the Internet is on this port, it will be forwarded to the indicated local IP address.

10.4. Port Trigger

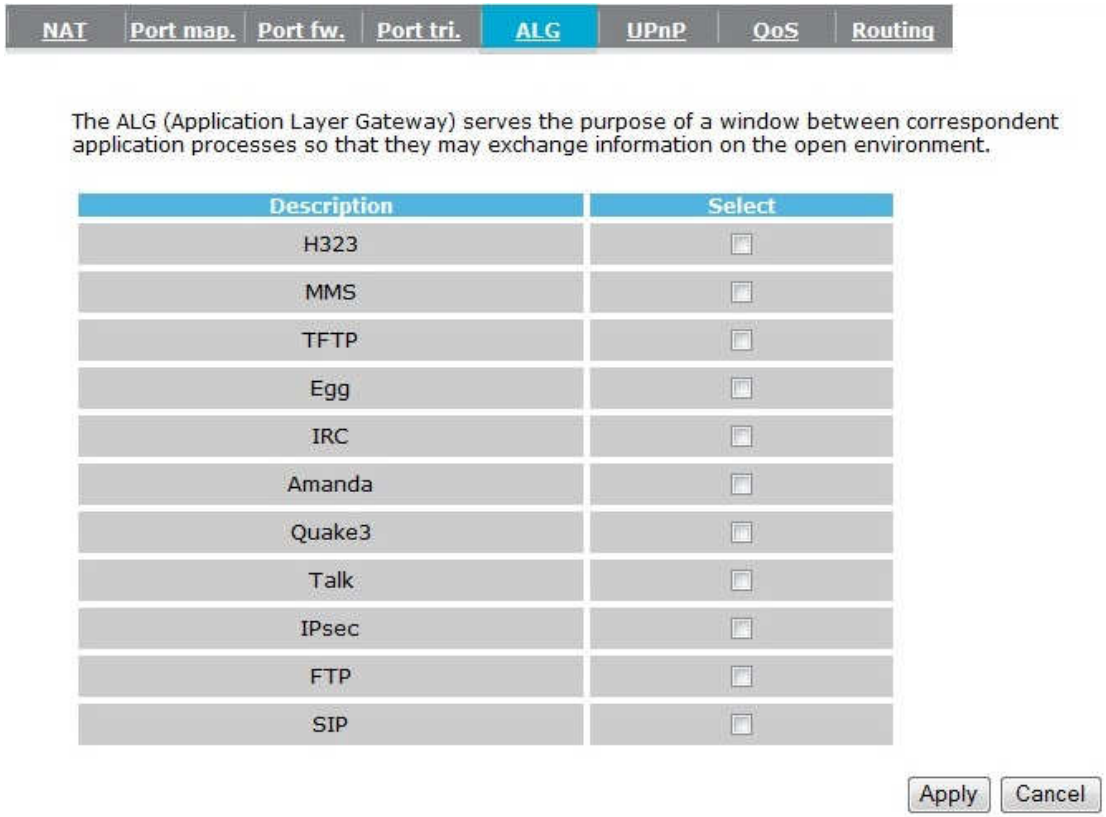
If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. Port Trigger will be required for these applications to work.



Port Trigger	
Enable Port Forwarding	Check this box to enable the Port Trigger feature.
Popular applications	This is a list of some common applications with preset settings. Select the application and click **Add** to automatically enter the settings.
Trigger port	This is the outgoing (outbound) port numbers for this application.
Trigger type	Select whether the application uses TCP, UDP or Both types of protocols for outbound transmissions.
Public Port	These are the inbound (incoming) ports for this application.
Public type	Select whether the application uses TCP, UDP or Both types of protocols for inbound transmissions.

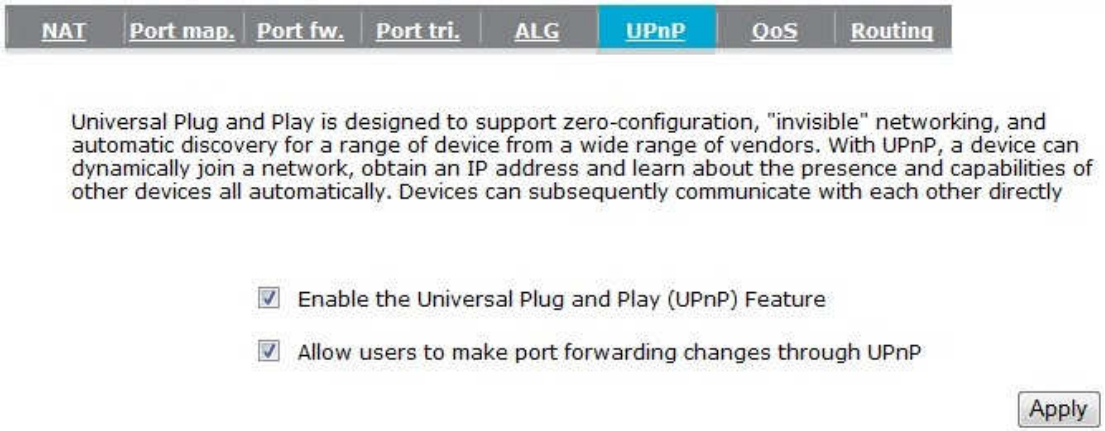
10.5. Application Layer Gateway (ALG)

Certain applications may require the use of the ALG feature to function correctly. If you use any of the applications listed on the table below, select the feature and click Apply.



10.6. Universal Plug and Play (UPnP)

The UPnP function allows automatic discovery and configuration of UPnP enabled devices on your network. It also provides automatic port forwarding for supported applications to seamlessly bypass the Firewall.

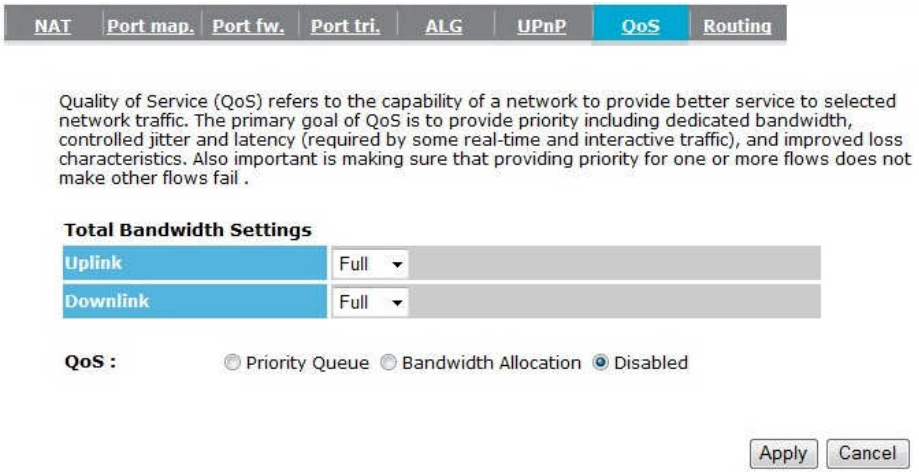


Universal Plug and Play (UPnP)	
Enable the UPnP Feature	Check this box to enable the UPnP feature to allow supported devices to be visible on the network.
Allow users to make port forwarding changes through UPnP	Check this box to allow applications to automatically set their port forwarding rules to bypass the firewall without any user set up.

10.7. Quality of Service (QoS)

QoS allows you to control the priority that the data is transmitted over the Internet, or to reserve a specific amount of Internet bandwidth. This is to ensure that applications get enough Internet bandwidth for a good user experience.

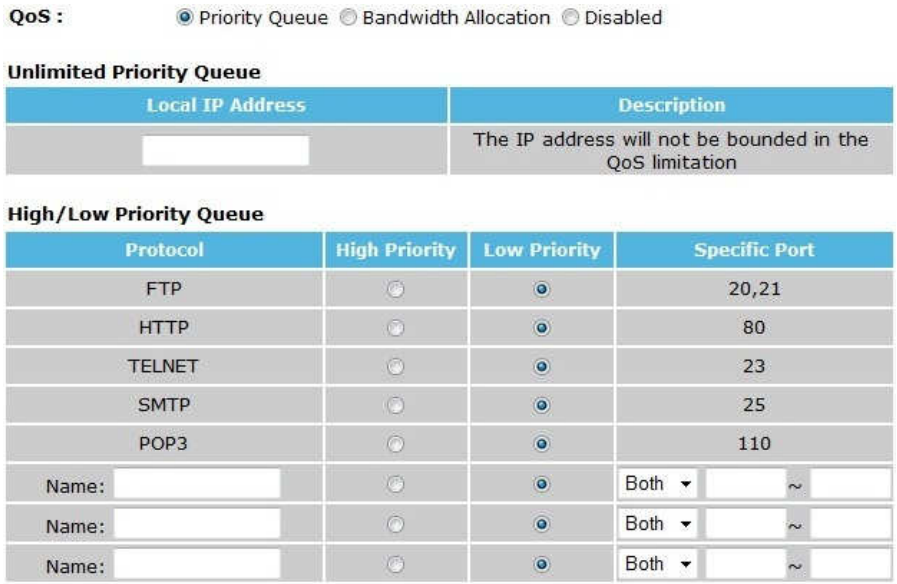
In order for this feature to function properly, the user should first set the Uplink and Downlink bandwidth provided by your Internet Service Provider.



Total Bandwidth Settings	
Uplink	Set the Uplink bandwidth provided by your Internet Service Provider.
Downlink	Set the Downlink bandwidth provided by your Internet Service Provider.
Priority Queue	Sets the QoS method to Priority Queue.
Bandwidth Allocation	Sets the QoS method to Bandwidth Allocation.
Disabled	Disables the QoS feature.

Priority Queue Method

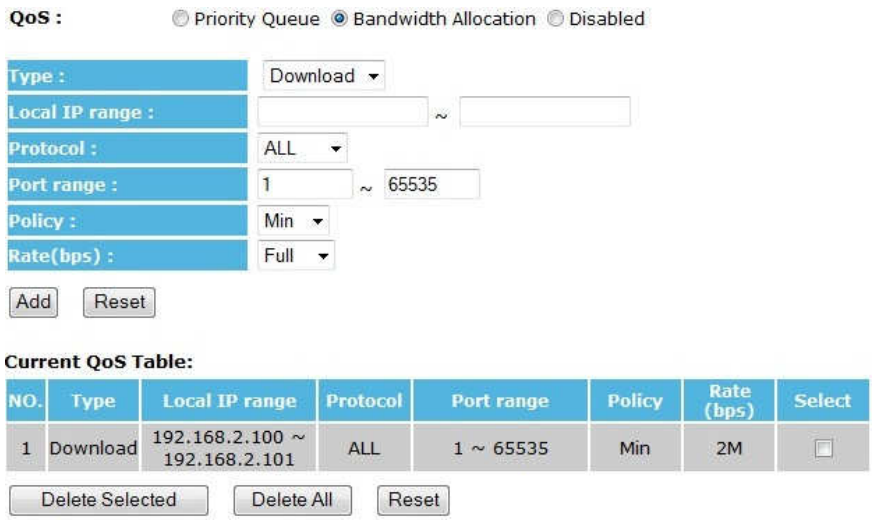
Bandwidth priority is set to either High or Low. The data transmissions in the High Priority queues will be processed first.



Unlimited Priority Queue	
Local IP Address	The computer with this IP Address will not be bound by the QoS rules.
High / Low Priority Queue	
Protocol	The type of network protocol.
High / Low Priority	Sets the protocol to High or Low priority.
Specific Port	Each protocol uses a specific port range. Please specify the ports used by this protocol.

Bandwidth Allocation Method

You can set the **maximum** amount of bandwidth a certain protocol will use at one time. Or you can set a **minimum** amount of bandwidth that will be guaranteed to a certain protocol.

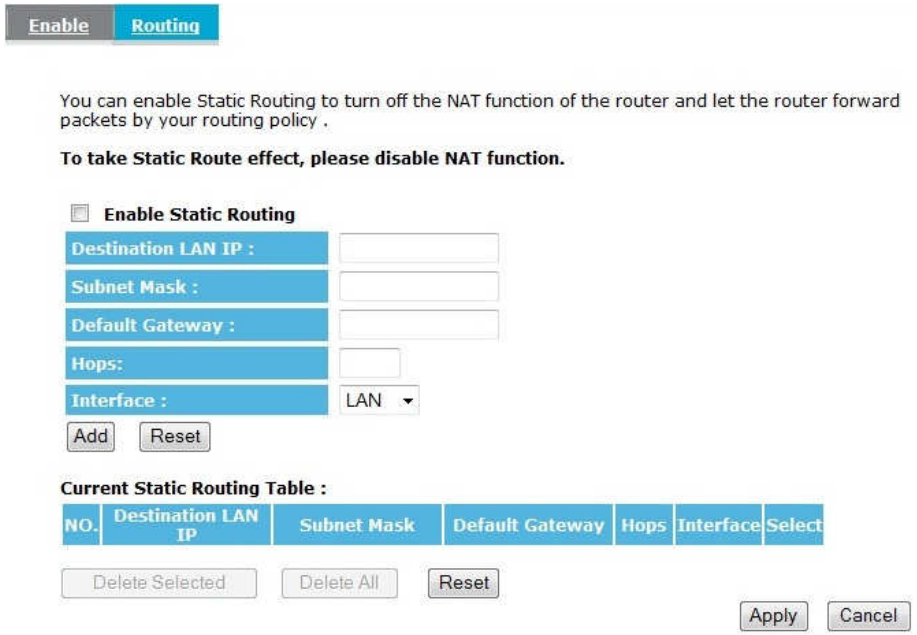


Bandwidth Allocation	
Type	Set whether the QoS rules apply to transmission that are Download, Upload or Both directions.
Local IP range	Enter the IP address range of the computers that you would like the QoS rules to apply to.
Protocol	Select from this list of protocols to automatically set the related port numbers.
Port range	Each protocol uses a specific port range. Specify the ports used by this protocol.
Policy	Choose whether this rule is to set a limit on the **Maximum** amount of bandwidth allocated to the specified protocol, or to set the guaranteed **Minimum** amount of bandwidth for the protocol.

10.8. Routing

If your wireless router is connected to a network with different subnets, this feature will allow the different subnets to communicate with each other.

Note: The NAT function needs to be disabled for the Routing feature to be enabled.



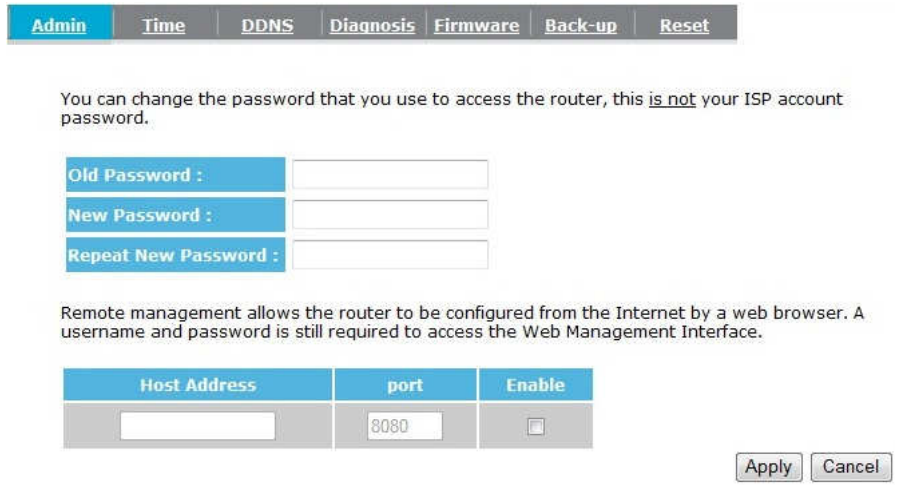
Static Routing	
Enable Static Routing	Check this box to enable the Static Router feature.
Destination LAN IP	Enter the IP address of the destination LAN.
Subnet Mask	Enter the Subnet Mask of the destination LAN IP address
Default Gateway	Enter the IP address of the Default Gateway for this destination IP and Subnet.
Hops	Specify the maximum number of Hops in the static routing rule.
Interface	Select whether the routing applies to LAN or WAN interfaces.

11. Tools

This section allows you to configure the Router's system settings.

11.1. Admin

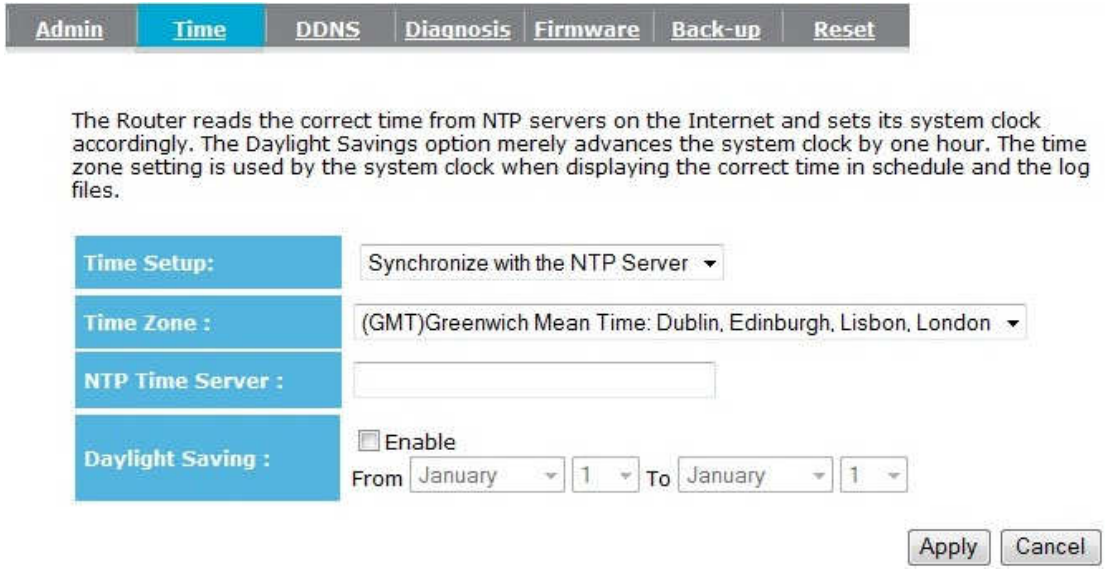
This page allows you to change the Router's password and to configure remote management.



Change Password	
Old Password	Enter the current password.
New Password	Enter your new password.
Repeat New Password	Enter your new password again for verification.
Remote Management	
Host Address	You can only perform remote management from the specified IP address. Leave blank to allow any host to perform remote management.
Port	Enter the port number you want to accept remote management connections.
Enable	Tick to Enable the remote management feature.

11.2. Time

This page allows you to configure the system time.

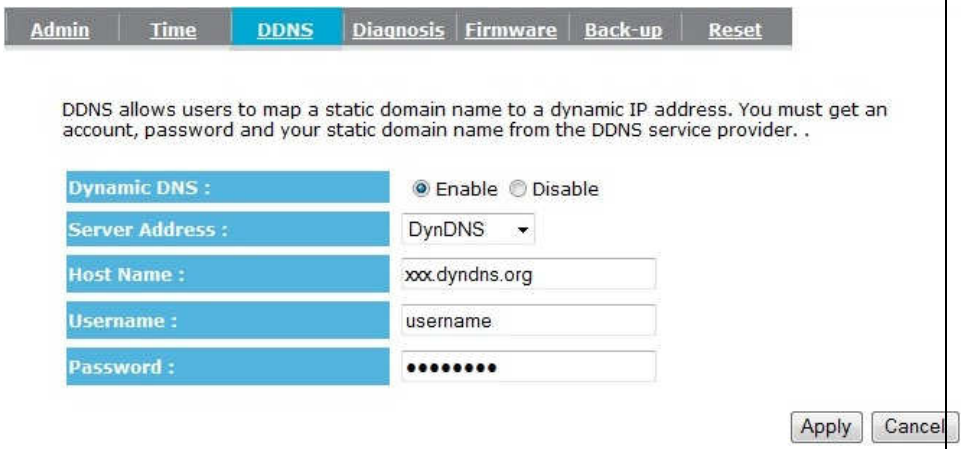


Time	
Time Setup	Select the method you want to set the time.
Time Zone	Select the time zone for your current location.
NTP Time Server	Enter the address of the Network Time Protocol (NTP) Server to automatically synchronize with a server on the Internet.
Daylight Savings	Check whether daylight savings applies to your area.

11.3. Dynamic DNS (DDNS)

This free service is very useful when combined with the *Virtual Server (Port Forwarding)* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.



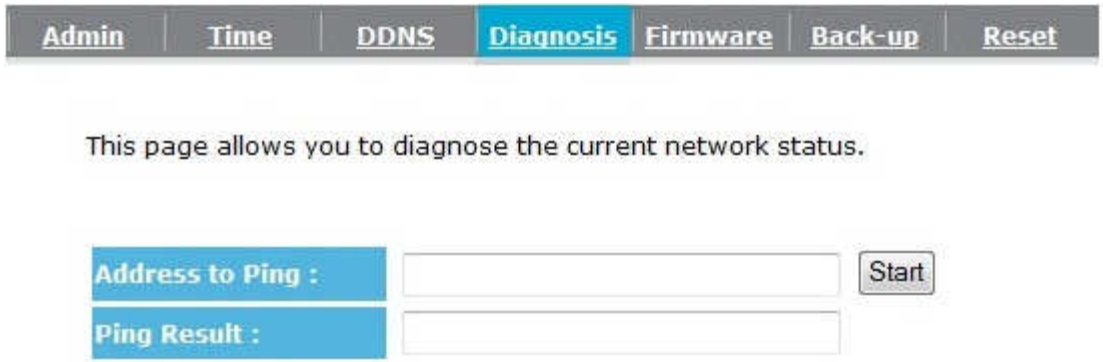
DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, follow the Service provider's procedure to obtain your desired Domain name.
3. Enter your DDNS data on the device's DDNS screen, and enable the DDNS feature.
4. The Wireless Router will automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS	
Dynamic DNS	Tick this box to Enable the DDNS feature.
Server Address	Select the list of Dynamic DNS homes you would like to use from this list.
Username / Password	Enter the Username and Password of your DDNS account.

11.4. Diagnosis

This page allows you to determine if the Router has an active Internet connection.



Diagnosis	
Address to Ping	Enter the IP address you would like to see if a successful connection can be made.
Ping Result	The results of the Ping test.

11.5. Firmware

The firmware (software) used by the Router can be upgraded using your Web Browser.

To perform the Firmware Upgrade:

1. Click the **Browse** button and navigate to the location of the firmware file.
2. Select the firmware file. Its name will appear in the *Upgrade File* field.
3. Click the **Apply** button to start the firmware upgrade.

Note: The Wireless Router is unavailable during the upgrade process and must restart when the upgrade is completed. Any connections to or through the Wireless Router will be lost during the upgrade.

Emergency Upgrade

If the firmware upgrade fails, you may enter the Emergency Upgrade WEB page.

1. Enter IP address: **192.168.99.9** on a web browser to enter the Emergency Upgrade WEB page.

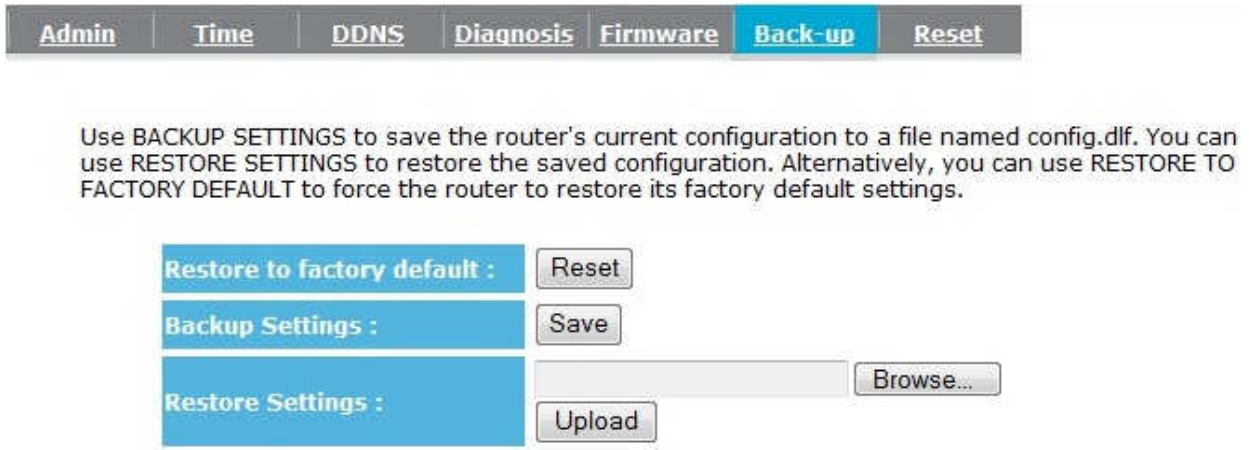
Note: You will need to configure your desktop or laptop to have an IP address of 192.168.99.8 or in the 192.168.99.X range. Refer to chapter 2 for more details on how to change the IP address of your desktop or laptop.

2. Click the [**Browse**] button and navigate to the location of the upgrade file and then click [**Upload**].

3. Wait for firmware upgrade and reboot the device.

4. You can access the device again after the emergency firmware upgrade has been completed.

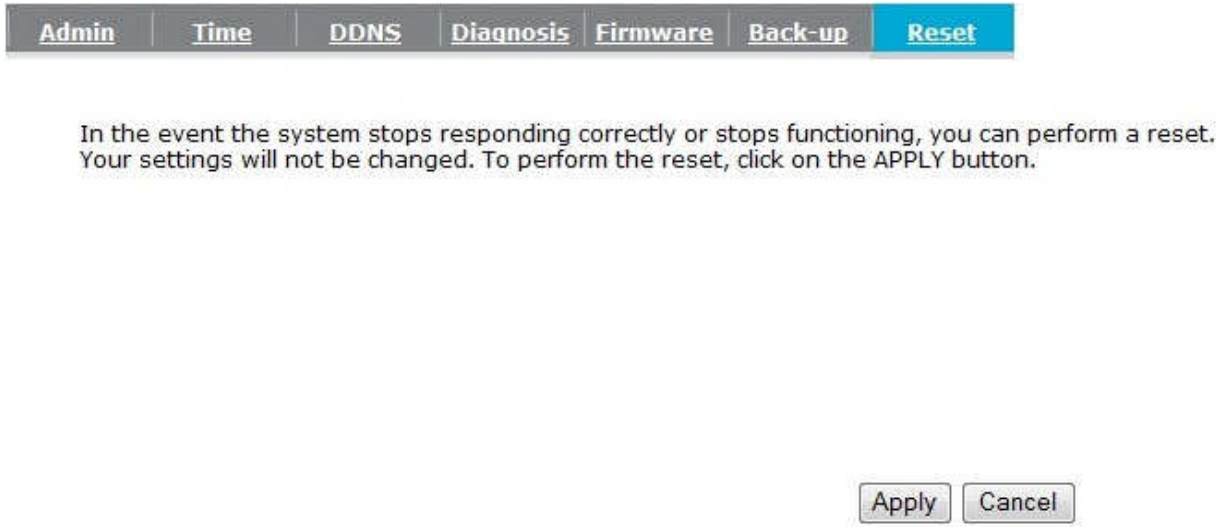
11.6. Back-up



Back-up	
Restore to factory default	Restores the Router to its factory default settings.
Backup Settings	Saves the Router's current configuration settings to a file.
Restore Settings	Restores a previously saved configuration file. Click **Browse** to select the file. Then click **Upload** to load the settings.

11.7. Reset

This page allows you to reset (restart) the Router. The current configuration settings will not be lost.



Appendix A – FCC Interference Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix B – IC Interference Statement

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

2011/August/Rev1.0